# Certificate Practice Statement

| | |
|---|---|
| Version: | 1.2.1 |
| Date: | 18-08-2020 |
| Status: | Final |
| Classification: | Public |

# 1. Introduction

Ensured is a Certification Authority (CA) that issues high quality and highly trusted digital Certificates to entities including private and public companies and individuals in accordance with the Ensured CPS. In its role as a CA, Ensured performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital certificate. Sectigo CA infrastructure is used for generating and signing Certificates and for the maintenance, issuance and publication of Certificate Revocation Lists (CRL's) for users within the Ensured PKI.

## 1.1 Overview

Ensured conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") published by the Certificate Authority/Browser Forum ("CA/B Forum") at https://cabforum.org. In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this document.

In case multiple or alternative methods or options are possible by the Baseline Requirements or EV Guidelines in order to perform a certain task and/or multiple or alternative methods or options are offered in order to comply to those Requirements and Guidelines, Ensured reserves the right to choose any of the methods or options applicable at any time and may choose to change its procedures at all times and decide to do so on a case to case basis.

Ensured meets the Adobe Approved Trust List Technical Requirements (AATL).

The CPS is only one of a set of documents relevant to the provision of Certification Services by Ensured and that the list of documents contained in this clause are other documents which this CPS will from time to time mention, although this is not an exhaustive list. The document name, location of and status, whether public or private, are detailed below.

| Document | Status | Location |
|---|---|---|
| Ensured CPS | Public | www.ensured.com/repository |
| General Conditions | Public | www.xolphin.com/terms |
| Privacy Statement | Public | www.ensured.com/privacy |
| ISMS | Private | |

## 1.2 Document Name and Identification

This document is the Ensured Certification Practice Statement (CPS). It outlines the legal, commercial and technical principles and practices that Ensured and Sectigo employ in providing certification services that include, but are not limited to, approving, issuing, using and managing of Digital Certificates and in maintaining an X.509 Certificate based public key infrastructure (PKIX) in accordance with the Certificate Policies determined by Sectigo. It also defines the underlying certification processes for Subscribers and describes Ensured's repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Ensured PKI.

This document is approved for publication on April 5, 2018 by the Ensured Policy Authority (EPA). The following revisions were made by the original document.

## 1.3 PKI Participants

This section identifies and describes some of the entities that participate within the Ensured PKI. Ensured conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

### 1.3.1 Certification Authorities

In its role as a CA, Ensured provides Certificate services in cooperation with Sectigo within the Ensured PKI. The Ensured CA will:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Repository,
- Issue and publish Certificates in a timely manner in accordance with the issuance times set out in this CPS,
- Upon receipt of a valid request to revoke the Certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a Certificate issued for use within the Ensured PKI,

- Publish CRLs on a regular basis, in accordance with the provisions described in this CPS,
- Distribute issued Certificates in accordance with the methods detailed in this CPS,
- Update CRLs in a timely manner as detailed in this CPS,
- Notify Subscribers via email of the imminent expiry of their Ensured issued Certificate (for a period disclosed in this CPS).

#### 1.3.1.1 Ensured

Ensured is a Certification Authority (CA) that issues PDF-Signing and Microsoft Document Signing Certificates. Ensured conforms to the Adobe Approved Trust List Technical Requirements and the WebTrust for Certification Authorities requirements.

#### 1.3.1.2 Sectigo

Sectigo is a Certification Authority (CA) that issues high quality and highly trusted digital Certificates to entities including private and public companies and individuals in accordance with the Sectigo CPS. In delivering its PKI services Sectigo complies in all material respects with high-level international standards including those on Qualified Certificates pursuant to the European Directive 99/93 and the relevant law on electronic signatures and all other relevant legislation and regulation. Sectigo extends, under agreement, membership of its PKI to approved third parties known as Registration Authorities. The international network of Sectigo RAs share Sectigo's policies and practices and CA infrastructure to issue Sectigo digital Certificates, or if appropriate, private labelled digital certificates.

### 1.3.2 Registration Authorities

Ensured does act as a Registration Authority for Certificates it issues

### 1.3.3 Subscribers (End Entities)

Subscribers of Ensured services are individuals or companies that use PKI in relation with Ensured supported transactions and communications. Subscribers are parties that are identified in a Certificate and hold the private key corresponding to the public key listed in the Certificate. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant for the services of Ensured.

### 1.3.4 Relying Parties

Relying Parties use PKI services in relation with various Ensured Certificates for their intended purposes and may reasonably rely on such Certificates and/or digital signatures verifiable with reference to a public key listed in a Subscriber Certificate. Because not all Certificate products are intended to be used in an e-commerce transaction or environment, parties who rely on Certificates not intended for e-commerce do not qualify as a Relying Party. Please refer to section Certificate Usage of this CPS to determine whether a particular product is intended for use in e-commerce transactions.

To verify the validity of a digital Certificate they receive, relying parties must refer to the CRL or Online Certificate Status Protocol (OCSP) response prior to relying on information featured in a Certificate to ensure that Ensured has not revoked the Certificate. The CRL location is detailed within the Certificate. OCSP responses are sent through the OCSP responder.

### 1.3.5 Other Participants

Xolphin B.V. and Ensured B.V. are 100% subsidiaries and complement each other in performing their activities at operational level. While Xolphin (as a Registration Authority) focusses on SSL Certificates and validation services for Certificate Authorities, Ensured (as a Certificate Authority) specializes in digitally signing, identification and authentication services. Because of overlap in operational activities, both entities make use of the same pool of professional trusted employees when needed.

## 1.4 Certificate Usage

A digital Certificate is formatted data that cryptographically binds an identified Subscriber with a public key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transactions. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

Ensured currently offers a portfolio of digital Certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications, including but not limited to secure email,

protection of online transactions and identification of persons, whether legal or physical, or devices on a network or within a community.

Ensured may update or extend its list of products, including the types of Certificates it issues, as it sees fit. The publication or updates of the list of Ensured products creates no claims by any third party.

### 1.4.1 Appropriate Certificate Uses

As detailed in this CPS in Appendix D, Ensured offers a range of distinct Certificate types. The different Certificate types have differing intended usages and differing policies. Pricing and Subscriber fees for the Certificates are made available on the relevant official Ensured websites. The maximum warranty associated with each Certificate is set forth in detail in the section Insurance or Warranty Coverage for End-Entities of this CPS.

As the suggested usage for a digital Certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific Certificate. Revoked Certificates are appropriately referenced in CRLs and published in Ensured directories.

**PDF-Signing Certificates**

PDF-Signing Certificates are used to authenticate documents. With Time-stamping the document can be authenticated beyond the validity period of the certificate.

### 1.4.2 Prohibited Certificate Uses

Certificates are prohibited from being used to the extent that the use is inconsistent with applicable law. DV Certificates are not for use as a means of providing identity assurance. Certificates are prohibited from being used as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe damage to persons or property.

## 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 Ensured CPS.

### 1.5.1 Organization Administering the Document

Ensured maintains this CPS, related agreements and Certificate policies referenced within this document. Certificate policies are maintained by the Ensured Policy Authority.

### 1.5.2 Contact Person

The Ensured Certificate Policy Authority (EPA) may be contacted at the following address:

Ensured B.V.
Rogier van der Weydestraat 2
1817 MJ Alkmaar
The Netherlands
Tel: + 31(0)800 3678 733

URL: www.ensured.com
Email: legal@ensured.com

### 1.5.3 CPS Suitability, Amendments and Publication

The Ensured Certificate Policy Authority is responsible for determining the suitability of certificate policies illustrated within the CPS. The EPA is responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition. Upon the Certificate Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the Ensured repository (available www.ensured.com/repository), with thirty days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

Revisions not denoted "significant" shall be those deemed by the CA's Policy Authority to have minimal or no impact on

subscribers and relying parties using Certificates and CRL's issued by CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS. Controls are in place to reasonably ensure that the Ensured CPS is not amended and published without the prior authorization of the Ensured Certificate Policy Authority.

### 1.5.4 CPS Approval Procedures

This CPS and any subsequent changes, amendments, or addenda, shall be approved by the Ensured Certificate Policy Authority (EPA).

## 1.6 Definitions and Acronyms

The list of definitions and acronyms located in this section are for use within the Ensured CPS.

### 1.6.1 Acronyms

See Appendix A in this CPS for the acronyms applicable to this CPS.

### 1.6.2 Definitions

See Appendix B in this CPS for the definitions applicable to this CPS.

# 2. Publication and repository responsibilities

Ensured publishes this CPS, Certificate terms and conditions, the Relying Party Agreement and copies of all Subscriber Agreements in the official Ensured Repository at www.ensured.com/repository. The Ensured Certificate Policy Authority maintains the Ensured Repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section Audit Logging Procedures of this CPS.

Published critical information may be updated from time to time as prescribed in this CPS. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

## 2.1 Repositories

Ensured publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices, references within this CPS, as well as any other information it considers essential to its services. The Repository may be accessed at www.ensured.com/repository.

## 2.2 Publication of Certification Information

The Ensured Certificate services and the Repository are accessible through several means of communication:

- On the web: www.ensured.com
- By email: legal@ensured.com
- By phone: +31(0)800 3678733, + 31(0)88 7757750
- By mail:

Ensured B.V.
Compliance Department
Rogier van der Weijdestraat 2
1817 MJ Alkmaar
The Netherlands

## 2.3 Time or Frequency of Publication

Issuance and revocation information regarding Certificates will be published as soon as possible. Updated or modified versions of Subscriber Agreements and Relying Party Agreements are usually published within seven days after approval. Updated or modified versions of the Ensured CPS are published in accordance with section Amendments of this CPS. For CRL issuance frequency, see section CRL Issuance Frequency of this CPS.

## 2.4 Access Controls on Repositories

Information published in the Repository is public information. Ensured has logical- and phisical access control and version control measures in place to prevent unauthorized persons from adding, deleting, or modifying repository entries.

### 2.4.1 Conditions of Usage of the Ensured Repository and Website

Parties (including Subscribers and Relying Parties) accessing the Ensured Repository (www.ensured.com/repository) and official website(s) agree with the provisions of this CPS and any other conditions of usage that Ensured may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by using an Ensured issued Certificate.

Failure to comply with the conditions of usage of the Ensured Repository and website may result in terminating the relationship between Ensured and the party.

## 2.5 Accuracy of Information

Ensured, recognizing its trusted position, makes all reasonable efforts to ensure that parties accessing the Repository receive accurate, updated and correct information. Ensured, however, cannot accept any liability beyond the limits set in this CPS and the Ensured insurance policy.

# 3. Identification and authentication

Ensured offers different Certificate types to make use of SSL and S/MIME technology for secure online transactions and secure email respectively. Prior to the issuance of a Certificate, Ensured will validate an application in accordance with this CPS that may involve the request by Ensured to the Applicant for relevant official documentation supporting the application.

## 3.1 Naming

### 3.1.1 Types of Names

Ensured issues Certificates with non-null subject DNs. The constituent elements of the subject DN conform with ITU X.500.

Ensured does not issue pseudonymous Certificates except as detailed in section Anonymity or Pseudonymity of Subscribers of this CPS.

Server authentication Certificates in general include entries in the subjectAlternateName (SAN) extension which are intended to be relied upon by relying parties.

### 3.1.2 Need for Names to be Meaningful

Ensured puts meaningful names in both the subjectDN and the issuerDN extensions of Certificates. The names in the Certificates identify the subject and issuer respectively.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

Ensured does not issue pseudonymous Certificates for server authentication, code-signing, PDF-signing or email use, but does issue some Certificates solely for client authentication where the names in the subject of the Certificate are meaningful only within the scope of the application with which they are issued to be used and are not generally meaningful outside that scope.

### 3.1.4 Rules for Interpreting Various Name Forms

The name forms used in Certificate subjectDNs and issuerDNs conform to a subset of those defined and documented in RFC 2253 and ITU-T X.520.

### 3.1.5 Uniqueness of Names

Ensured does not in general enforce uniqueness of subject names. However, Ensured assigns Certificate serial numbers that appear in Ensured Certificates. Assigned serial numbers are unique. Ensured generates at least 64-bit serial numbers. These numbers are the output of a CSPRNG. We have a separate uniqueness check that verifies that serial numbers are never re-used.

### 3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers and Applicants may not request Certificates with content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated in this CPS, Ensured does not verify an Applicant's or Subscriber's right to use a trademark. Ensured does not resolve trademark disputes. Ensured may reject any application or revoke any Certificate that is part of a trademark dispute.

Ensured does check subject names against a limited number of trademarks and brand names which are perceived to be of high value. A match between a part of the subject name and one of these high value names triggers a more careful examination of the subject name and Applicant.

## 3.2 Initial Identity Validation

This section contains information about Ensured's identification and authentication procedures for registration of subjects such as Applicants, CAs, and other participants. Ensured may use any legal means of communication or investigation to validate the identity of these subjects. From time to time, Ensured may modify the requirements related to application information to respond to Ensured's requirements, the business context of the usage of a digital Certificate, other industry requirements, or as prescribed by law.

### 3.2.1 Method to Prove Possession of Private Key

Verification of a digital signature is used to determine that:

- the private key corresponding to the public key listed in the signer's Certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

The usual means by which Ensured accepts signed data from an Applicant to prove possession of a private key is in the receipt of a PKCS#10 Certificate Signing Request (CSR).

### 3.2.2 Authentication of Organization Identity

Authentication of an organization identity is performed through the validation processes specified below, and depends on the type of Certificate. Applications for Ensured Certificates are supported by appropriate documentation to establish the identity of an Applicant.

The following elements are critical information elements for an Ensured Certificate issued to an Organization. Those elements marked with PUBLIC are present within an issued Certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country, email (PUBLIC)
- VAT-number (if applicable)
- Company / DUNS number (if available)
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber Agreement, signed (if applying out of bands)

#### 3.2.2.1 Authentication of Organization Identity for Document Signing Certificates

Ensured verifies the identity and address of the Applicant in accordance with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (commonly referred to as the Baseline Requirements), using documentation that is provided by, or through communication with at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA, or;
4. An attestation letter;

Ensured MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, Ensured MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that Ensured determines to be reliable.

If the Subject Identity Information in the certificate is to include a DBA or Trade Name, Ensured shall verify the Applicant's right to use such DBA/Trade Name using number 1, 2, or 4 above, or:

1. Communication directly with a government agency responsible for the management of such DBAs or trade names, or;
2. A utility bill, bank statement, credit card statement, government issued tax document, or other form of identification that Ensured determines to be reliable.

#### 3.2.2.2 PDF Signing Certificates

Applicant organizational identity is validated in accordance with the CA/Browser Forum WebTrust for Certification Authorities guidelines.

### 3.2.3 Authentication of Individual Identity

Authentication of an individual identity is performed through the validation processes specified below, and depends on the type of Certificate. Applications for Ensured Certificates are supported by appropriate documentation to establish the identity of an Applicant.

The following elements are critical information elements for an Ensured Certificate issued to an individual entity:

- Legal Name of the Individual (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country, email (PUBLIC)
- VAT-number (if applicable)
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber Agreement, signed (if applying out of bands)

#### 3.2.3.1 Authentication of Individual Identity for Document Signing Certificates

In addition to the verification of domain control using the procedures listed above, if the Applicant is a natural person, Ensured verifies the identity and address of the Applicant in accordance with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (commonly referred to as the Baseline Requirements), using:

1. Verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government issued photo ID (passport, drivers license, military ID, national ID or equivalent document type)
2. Verify the Applicant's address using a form of identification that Ensured determines to be reliable such as a government ID, utility bill, or bank or credit card statement. Ensured MAY rely on the same government issued ID that was used to verify the Applicant's name.

Ensured may accept or require, at its discretion, other official documentation supporting an application, possibly including, but not limited to, requiring face to face verification of the Applicant's identity before an authorized agent of Sectigo, an attorney, a CPA, a Latin notary, a notary public or equivalent.

#### 3.2.3.2 PDF Signing Certificates

Applicant individual identity is validated in accordance with the CA/Browser Forum WebTrust for Certification Authorities guidelines

### 3.2.4 Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this CPS, Ensured shall not be responsible for non-verified Subscriber information submitted to Ensured, or the Ensured directory or otherwise submitted with the intention to be included in a Certificate, except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93.

### 3.2.5 Validation of Authority

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate. Validation of authority is dependent on the type of Certificate requested and is performed in accordance with section Application Validation of this CPS.

#### 3.2.5.1 S/MIME / Client Certificates / PDF signing Certificates

The request is verified via email sent to the email address to be contained in the Certificate Subject.

### 3.2.6 Criteria for Interoperation

Ensured may provide services allowing for another CA to operate within, or interoperate with, its PKI. Such interoperation may include cross-certification, unilateral certification, or other forms of operation. Ensured reserves the right to provide interoperation services and to interoperate with other CAs; the terms and criteria of which are to be set forth in the applicable agreement.

### 3.2.7 Application Validation

Prior to issuing a Certificate or issuing a Site Seal, Ensured employs controls to validate the identity of the Subscriber information featured in the Certificate application. Such controls are indicative of the product type:

#### 3.2.7.1 Personal Secure Email Certificate

The only identifying information in the subject DN is the email address of the Subscriber. Ensured validates the right for the Applicant to use the submitted email address. This is achieved through the delivery via a challenge and response made to the email address submitted during the Certificate application.

Ensured validates that the Applicant holds the private key corresponding with a public key to be included in the Certificate by utilizing an online enrollment process whereby Ensured facilitates the Subscriber generating its key-pair using a specially crafted web page. The key pair is generated in the Subscriber's computer. The private key is not exported or transferred from the Subscriber's computer as part of the application process.

#### 3.2.7.2 Corporate Secure Email Certificate

Corporate Secure Email Certificates will only be issued to email addresses within approved domain names. The Applicant must first submit a domain name to Ensured and appropriate domain name ownership, or right to use a domain name, validation takes place in accordance with the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted. Upon successful validation of a submitted domain name Ensured allows the Applicant to utilize email addresses within the domain name.

The administrator will submit the secure email Certificate end-entity information on behalf of the end-entity. An email is then delivered to the end-entity containing unique login details to online Certificate generation and collection facilities. Once logged into the online Certificate generation and collection facilities, the end-entity's browser creates a public and private key pair. The public key is submitted to Ensured who will issue a Corporate Secure Email Certificate containing the public key. Ensured then validates using an automated cryptographic challenge that the Applicant holds the private key associated with the public key submitted during this automated application process. If the automated challenge is successful, Ensured will release the digital Certificate to the end-entity Subscriber.

## 3.3 Identification and Authentication for Re-Key Requests

Ensured rekeys on:

- Replacement, which is when a Subscriber wishes to change some (or none) of the subject details in an already issued Certificate and may (or may not) also wish to change the key associated with the new Certificate; and
- Renewal, which is when a Subscriber wishes to extend the lifetime of a Certificate which has been issued they may at the same time vary some (or none) of the subject details and may also change the key associated with the Certificate.

In both cases, Ensured requires the Subscriber to use the same authentication details which they used in a previous purchase of a Certificate on the same account. In either case, if any of the subject details are changed during the replacement or renewal process then the subject must be reverified.

### 3.3.1 Identification and Authentication for Routine Re-Key

As stated above - in both cases, Ensured requires the Subscriber to use the same authentication details which they used in a previous purchase of the Certificate on the same account.

### 3.3.2 Identification and Authentication for Re-Key after Revocation

Ensured does not routinely permit rekeying (or any form of reissuance or renewal) after revocation. Revocation is a terminal event in the Certificate lifecycle.

Where a request for replacement or renewal of a Certificate after revocation is considered, Ensured requires the Subscriber to authenticate itself using the original authentication details used on a purchase of a certificate on the same account. However, this may be varied, or rekeying may be refused after revocation, where the exact circumstances and reasons for which the Certificate was revoked are not adequately explained. Reissuance or replacement after revocation is solely at Ensured's discretion.

## 3.4 Identification and Authentication for Revocation Request

### 3.4.1 Revocation at the Subscriber's request

The Subscriber must either be in possession of the authentication details which were used to purchase a previous Certificate on the same account OR the Subscriber must be able to send an S/MIME email signed with the private key associated with the Certificate.

### 3.4.2 Revocation at the CA's request

Ensured does not revoke Certificates at the request of other CAs. Ensured can and does revoke Subscriber Certificates for cause as set out in section Certificate Revocation and Suspension of this CPS, but identification and authentication is not required in these cases.

Ensured employs the following procedure for authenticating a revocation request:

- The revocation request must be sent by the administrator contact associated with the Certificate application. Ensured may if necessary also request that the revocation request be made by either / or the organizational contact and billing contact.
- Upon receipt of the revocation request Ensured will request confirmation from the known administrator out of bands contact details, either by telephone or by email.
- Ensured validation personnel will then command the revocation of the Certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

# 4. Certificate life-cycle operational requirements

This section describes the Certificate application process, including the information required to make and support a successful application. Additionally, this section describes some of the requirements imposed upon Subscribers, and other participants with respect to the life-cycle of a Certificate.

The validity period of Ensured Certificates varies dependent on the Certificate type, but typically, a Certificate will be valid for either 1 year, 2 years or 3 years. Ensured reserves the right to, at its discretion, issue Certificates that may fall outside of these set periods.

The following steps describe the milestones to issue a digital Certificate:

1. The Applicant fills out the online request on Ensured's website and the Applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organizational information, country code, verification method and billing information.
2. The Applicant accepts the online Subscriber Agreement.
3. The Applicant submits the required information to Ensured.
4. Ensured verifies the submitted information using third party databases and Government records
5. Upon successful validation of the application information, Ensured may issue the Certificate to the Applicant or should the application be rejected, Ensured will alert the Applicant that the application has been unsuccessful.
6. After the Certificate has been issued the Applicant pays the Certificate fees.
7. Renewal is conducted as per the procedures outlined in this CPS and the official Ensured websites.
8. Revocation is conducted as per the procedures outlined in this CPS.

## 4.1 Certificate Application

A Certificate request can be done according to the following means:
On-line: Via the Web (https). The Certificate Applicant submits an application via a secure online link according to a procedure provided by Ensured. Additional documentation in support of the application may be required so that Ensured verifies the identity of the Applicant. The Applicant submits to Ensured such additional documentation. Upon verification of identity, Ensured issues the Certificate and sends a notice to the Applicant. The Applicant downloads and installs the Certificate to its device. The Applicant must notify Ensured of any inaccuracy or defect in a Certificate promptly after receipt of the Certificate or earlier notice of informational content to be included in the Certificate.

Ensured may at its discretion, accept applications via email/mail.

### 4.1.1 Who can Submit a Certificate Application

Generally, Applicants will complete the online forms made available by Ensured at the respective official websites. Under special circumstances, the Applicant may submit an application via email/mail; however, this process is available at the discretion of Ensured.

### 4.1.2 Enrolment Process and Responsibilities

All Certificate Applicants must complete the enrolment process, which may include:

- Generate an RSA or ECC key pair and demonstrate to Ensured ownership of the private key associated with the public key to be included in the Certificate through the submission of a valid PKCS#10 Certificate Signing Request (CSR) (or SPKAC request for certain client authentication or email Certificates)
- Make all reasonable efforts to protect the integrity and confidentiality of the private key.
- Submit to Ensured a Certificate application, including application information as detailed in this CPS, a public key corresponding to the private key of which they are in possession, and agree to the terms of the relevant Subscriber Agreement
- Provide proof of identity through the submission of official documentation as requested by Ensured during the enrolment process.

## 4.2 Certificate Application Processing

Certificate applications are submitted to Ensured. The Certificates are processed and issued by Ensured.

| Certificate Type | Enrolment Entity | Processing Entity | Issuing Authority |
|---|---|---|---|
| Ensured e-Sign PDF Signing Certificate | End Entity Subscriber | Ensured | Sectigo |
| Ensured e-Seal PDF Signing Certificate | End Entity Subscriber | Ensured | Sectigo |

### 4.2.1 Performing Identification and Authentication Functions

Upon receipt of an application for a digital Certificate and based on the submitted information, Ensured confirms the following information:

- The Certificate Applicant is the same person as the person identified in the Certificate request.
- The Certificate Applicant holds the private key corresponding to the public key to be included in the Certificate.
- The information to be published in the Certificate is accurate, except for non-verified Subscriber information.
- Any agents who apply for a Certificate listing the Certificate Applicant's public key are duly authorized to do so.

Ensured may use the services of a third party to confirm information on a business entity that applies for a digital Certificate. Ensured accepts confirmation from third party organizations, other third party databases, and government entities.

Ensured's controls may also include trade registry transcripts that confirm the registration of the Applicant company and state the members of the board, the management and directors representing the company.

Ensured may use any means of communication at its disposal to ascertain the identity of an organizational or individual Applicant. Ensured reserves right of refusal in its absolute discretion.

Ensured has a system in place which examines subject details, including domain names, for matches or near matches to some known high profile or pre-notified names that may indicate that a certificate is at a higher than normal risk of fraudulent applications being made and in those cases the certificate application is flagged for manual review.

### 4.2.2 Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a Certificate application Ensured approves an application for a digital Certificate.

If the validation of a Certificate application fails, Ensured rejects the Certificate application. Ensured reserves its right to reject applications to issue a Certificate to Applicants if, on its own assessment, by issuing a Certificate to such parties the good and trusted name of Ensured might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently reapply.

In all types of Ensured Certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Ensured of any changes that would affect the validity of the Certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but that have not yet been paid under the Subscriber Agreement.

### 4.2.3 Time to Process Certificate Applications

Ensured makes reasonable efforts to confirm Certificate application information and issue a digital Certificate within a reasonable time frame. The time frame is greatly dependent on the type of Certificate and Subscriber providing the necessary details and / or documentation in a timely manner. Upon the receipt of the necessary details and / or documentation, Ensured aims to confirm submitted application data and to complete the validation process and issue / reject a Certificate application within 1 working day. An exception is an EV Certificate application, which can take up to five working days.

From time to time, events outside of the control of Ensured may delay the issuance process, however Ensured will make every reasonable effort to meet issuance times and to make Applicants aware of any factors that may affect

issuance times in a timely manner.

#### 4.2.4 Certificate Authority Authorization

Ensured issues PDF signing Certificates only, Certificate Authority Authorization is not required.

## 4.3 Certificate Issuance

Ensured issues a Certificate upon approval of a Certificate application. A digital Certificate is deemed to be valid at the moment a Subscriber accepts it (refer to section Certificate Acceptance of this CPS). Issuing a digital Certificate means that Ensured accepts a Certificate application.

Ensured Certificates are issued to organizations or individuals.
Subscribers shall solely be responsible for the legality of the information they present for use in Certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

#### 4.3.1 CA Actions during Certificate Issuance

Ensured's automated systems receive and collate:

- evidence gathered during the verification process, and/or
- assertions that the verification has been completed according to the policy and internal documentation that sets out the acceptable means of verifying subject information.

Ensured's automated systems record the details of the business transaction associated with the submission of a Certificate request and the eventual issuance of a Certificate, one example of which is a sales process involving a payment.

Ensured's automated (and manual) systems record the source of, and all details submitted with, evidence of verification, having been performed either by external RAs or by Ensured's internal RA.

The correct authentication of verification evidence provided by external RAs is required before that evidence will be considered for Certificate issuance.

The only Certificates Ensured issues from its root CAs are intermediate CA Certificates and cross Certificates.

Our CA outsourced to Sectigo, has no facility for the automated signature of such Certificates, so this activity necessarily involves manual intervention by privileged users to sign such Certificates. Certificate issuance by the Root CA requires an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

#### 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Ensured notifies Subscriber of the issuance of a Certificate through delivery. Delivery of Subscriber Certificates to the associated Subscriber is dependent on the Certificate product type:

##### 4.3.2.1 Secure Server Certificates

Secure server Certificates are delivered via email and the Ensured Control Panel to the Subscriber using the administrator contact email address provided during the application process.

##### 4.3.2.2 Code Signing Certificates

Code Signing Certificates are delivered via email and the Ensured Control Panel to the Subscriber using the administrator contact email address provided during the application process.

##### 4.3.2.3 Secure Email Certificate: Personal Secure Email, Corporate Secure Email Certificates

Upon issuance of a Personal Secure Email Certificate, Corporate Secure Email Certificate the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original Certificate request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the private key corresponding to the public key submitted during application. Pending a successful challenge, the issued Certificate is installed automatically onto the Subscriber's

computer.

#### 4.3.2.4 PDF Signing Certificates

Upon issuance of a PDF Signing Certificate, the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link, and have the USB Token in place on the computer in question. The Subscriber's cryptographic service provider software is initiated to ensure the Token holds the private key corresponding to the certificate. Pending a successful challenge, the issued Certificate is installed automatically onto the Subscriber's USB Token.

### 4.3.3 Refusal to Issue a Certificate

Ensured reserves its right to refuse to issue a Certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Ensured reserves the right not to disclose reasons for such a refusal.

## 4.4 Certificate Acceptance

This section describes some of the actions by Subscriber in accepting a Certificate. Additionally, it describes how Ensured publishes a Certificate and how Ensured notifies other entities of the issuance of a Certificate.

### 4.4.1 Conduct Constituting Certificate Acceptance

An issued Certificate is either delivered via email/Ensured Control Panel, installed on a Subscriber's computer / hardware security module through an online collection method or delivered via certified mail on a password secured token. A Subscriber is deemed to have accepted a Certificate when:

- the Subscriber uses the Certificate, or
- 30 days pass from the date of the issuance of a Certificate

### 4.4.2 Publication of the Certificate by the CA

A Certificate is published through various means: (1) by Ensured making the Certificate available in the Repository; and (2) by Subscriber using the Certificate subsequent to Ensured's delivery of the Certificate to Subscriber.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Ensured provides notification of Certificate issuance to the following entities by the following means: Reseller Partner: Issued Subscriber PDF Signing Certificates applied for through a Reseller Partner on behalf of the Subscriber are made available in the Repository to the administrator contact of the Reseller Partner account. The corresponding hardware security module is shipped directly to the Subscriber.

## 4.5 Key Pair and Certificate Usage

This section is used to describe the responsibilities relating to the use of keys and Certificates.

### 4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties.

Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate. Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. Private Keys generated on a FIPS token cannot be exported. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

### 4.5.2 Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the Relying Party. Reliance on a digital signature should only occur if:

- the digital signature was created during the operational period of a valid Certificate and it can be verified by referencing a validated Certificate;
- the Relying Party has checked the revocation status of the Certificate by referring to the relevant CRLs and the Certificate has not been revoked;
- the Relying Party understands that a digital Certificate is issued to a Subscriber for a specific purpose and that the private key associated with the digital Certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the Certificate profile; and
- the digital Certificate applied for is appropriate for the application it is used in.

Reliance is accepted as reasonable under the provisions made for the Relying Party under this CPS and within the Relying Party agreement. If the circumstances of reliance exceed the assurances delivered by Sectigo under the provisions made in this CPS, the Relying Party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

## 4.6 Certificate Renewal

Certificate renewal means the issuance of a new Certificate to the Subscriber.

Depending on the option selected during application, the validity period of Ensured Certificates is 1, 2 or 3 years from the date of issuance and is detailed in the relevant field within the Certificate.
Renewal fees are detailed on the official Ensured websites and within communications sent to Subscribers approaching the Certificate expiration date.

### 4.6.1 Circumstance for Certificate Renewal

Ensured shall make reasonable efforts to notify Subscribers via e-mail of the imminent expiration of a digital Certificate. Notice shall ordinarily be provided within a 30-day period prior to the expiry of the Certificate.

### 4.6.2 Who May Request Renewal

Those who may request renewal of a Certificate include, but are not limited to, a Subscriber on behalf of itself. Ensured does not automatically renew Certificates.

### 4.6.3 Processing Certificate Renewal Requests

In order to process Certificate renewal requests, Ensured gets the Subscriber to reauthenticate itself. Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers. Ensured doesn't require that the Subscriber use the same key on the new application.

### 4.6.4 Notification of New Certificate Issuance to Subscriber

Notification to the Subscriber about the issuance of a renewed Certificate is given using the same means as a new Certificate, described in section Notification to Subscriber by the CA of Issuance of Certificate of this CPS.

### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Subscriber's conduct constituting acceptance of a renewal Certificate is the same as listed in section Conduct Constituting Certificate Acceptance of this CPS.

### 4.6.6 Publication of the Renewal Certificate by the CA

Publication of a renewed Certificate is performed through various means: (1) by Ensured making the Certificate available in the Repository; and (2) by Subscriber using the Certificate subsequent to Ensured's delivery of the Certificate to Subscriber.

### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Generally, Ensured does not notify other entities of a renewed Certificate. In limited circumstances, Ensured will notify other entities through the means described in section Publication of the Renewal Certificate by the CA of this CPS.

## 4.7 Certificate Rekey

This section is used to describe elements/procedures generating a new key pair and applying for the issuance of a new Certificate that certifies the new public key. Rekeying (or re-keying) a Certificate may comprise of creating a new Certificate with a new public key and serial number, while retaining the Certificate's subject information.

### 4.7.1 Circumstances for Certificate Re-Key

Certificate rekey will ordinarily take place as part of a Certificate renewal or Certificate replacement, as stated in section Initial Identity Validation of this CPS. Certificate rekey may also take place when a key has been compromised.

### 4.7.2 Who May Request Certificate Rekey

Those who may request a Certificate rekey include, but are not limited to, the Subscriber or Ensured at its discretion.

### 4.7.3 Processing Certificate Rekey Requests

Depending on the circumstances, the procedure to process a Certificate rekey may be the same as issuing a new Certificate. Under other circumstances, Ensured may process a rekey request by having the Subscriber authenticate its identity.

### 4.7.4 Notification of Rekey to Subscriber

Ensured will notify a Subscriber of a Certificate rekey by the means delineated in section Notification to Subscriber by the CA of Issuance of Certificate of this CPS.

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Subscriber's conduct constituting acceptance of a rekeyed Certificate is the same as listed in section Conduct Constituting Certificate Acceptance of this CPS.

### 4.7.6 Publication of the Re-Keyed Certificate by the CA

Publication of a re-keyed Certificate is performed by delivering it to the Subscriber and by Ensured using the LDAP server- a publicly accessible directory of client Certificates.

### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Generally, Ensured does not notify other entities of the issuance of a rekeyed Certificate. In limited circumstances, Ensured will notify other entities through the means described in section Publication of the Renewal Certificate by the CA of this CPS.

## 4.8 Certificate Modification

Ensured does not offer Certificate modification. Instead, Ensured will revoke the old Certificate and issue a new Certificate as a replacement.

### 4.8.1 Circumstance for Certificate Modification

Not applicable.

### 4.8.2 Who May Request Certificate Modification

Not applicable.

### 4.8.3 Processing Certificate Modification Requests

Not applicable.

### 4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

### 4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Ensured provides notification of Certificate issuance to the following entities by the following means:

End Entity Subscriber: Issued PDF Signing Certificates applied for through a Reseller Partner on behalf of the Subscriber are emailed to the administrator contact of the End Entity Subscriber account. End Entity Subscribers have control of issuance and collecting an issued Certificate from a request specific URL. Installation can be done directly on the FIPS-2 token on the moment of collecting.

Reseller Partner: Issued PDF Signing Certificates applied for through a Reseller Partner on behalf of the Subscriber are emailed to the administrator contact of the Reseller Partner account in BASE64 format without the corresponding private key

## 4.9 Certificate Revocation and Suspension

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. In other words, upon revocation of a Certificate, the operational period of that Certificate is immediately considered terminated. The serial number of the revoked Certificate will be placed within the CRL and remains on the CRL until sometime after the end of the Certificate's validity period.

Ensured does not utilize Certificate suspension.

### 4.9.1 Circumstances for Revocation

Ensured may revoke a digital Certificate if any of the following occur:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the Certificate;
- The Subscriber or Ensured has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- Either the Subscriber's or Ensured's obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or 'communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- There has been a modification of the information pertaining to the Subscriber that is contained within the Certificate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way;
- A Subscriber's Digital Certificate has not been issued in accordance with the policies set out in this CPS;
- The Subscriber has used the Subscription Service contrary to law, rule or regulation, or Ensured reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Certificate was issued as a result of fraud or negligence; or
- The Certificate, if not revoked, will compromise the trust status of Ensured.

### 4.9.2 Who can Request Revocation

A Subscriber or another appropriately authorized party can request revocation of a Certificate. Other parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, in the first instance, by email to legal@ ensured.com

### 4.9.3 Procedure for Revocation Request

A revocation request can be done via telephone or email via Ensured's regular contact information. For an emergency revocation outside of business hours Ensured should be contacted by phone.

Prior to the revocation of a Certificate, Ensured will verify that the revocation request has been:

- Made by the organization or individual entity that has made the Certificate application.
- Has been authenticated by the procedures in section Identification and Authentication for Revocation Request of this CPS.

### 4.9.4 Revocation Request Grace Period

The revocation request grace period ("Grace Period") means the period during which the Subscriber must make a revocation request. The Grace Period is defined in the Subscriber Agreement applicable to the individual Subscriber. In the event that a Grace Period is not defined in the Subscriber Agreement, Subscribers are required to request revocation within 24 hours after detecting the loss or compromise of the Private Key.

### 4.9.5 Time Within which CA Must Process the Revocation Request

For properly authenticated revocation requests received from the Subscriber to Ensured's systems, revocation will be reflected in the OCSP and in the CRLs within 24 hours.

### 4.9.6 Revocation Checking Requirement for Relying Parties

Parties relying on a digital Certificate must verify a digital signature at all times by checking the validity of a digital Certificate against the relevant CRL published or using the OCSP responder. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

Relying on an unverifiable digital signature may result in risks that the Relying Party, and not Ensured, assume in whole.

By means of this CPS, Ensured has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at www.ensured.com/repository or by contacting via out of bands means via the contact address as specified in the Contact Person section of this CPS.

### 4.9.7 CRL Issuance Frequency

CRLs for revocation of Ensured's Certificates are maintained and hosted by Sectigo and published on crl.ensuredca.com

to allow relying parties to verify a digital signature made using an Ensured issued digital Certificate. Each CRL contains entries for all revoked un-expired Certificates issued and is valid for 24 hours. CRL's are published every 24 hours and include a monotonically increasing sequence number for each CRL issued. Under special circumstances, new CRLs prior to the expiry of the current CRL may be published. All expired CRLs are archived for a period of 7 years or longer if applicable. For Code Signing Certificates revoked due to key compromise or that have been issued to unauthorized persons,certificate information on CRLs will be maintained for at least 20 years.

### 4.9.8 Maximum Latency for CRLs

The maximum latency for CRLs means the maximum time between the generation of CRLs and posting of the CRLs to the repository (i.e., the maximum amount of processing- and communication-related delays in posting CRLs to the repository after the CRLs are generated). Ensured does not employ a maximum latency for CRLs. Generally, however, CRLs are published within 1 hour.

### 4.9.9 On-Line Revocation/Status Checking Availability

In addition, Sectigo's systems are configured to generate and serve OCSP responses. This provides real-time information regarding the validity of the Certificate making the revocation information immediately available through the OCSP protocol. CRLs and OSCP are available 24/7 to anyone.

### 4.9.10 On-Line Revocation Checking Requirements

Sectigo manages the OCSP services on behalf of Ensured. Sectigo?s OCSP responses are either:

- Signed by the CA that issued the Certificates whose revocation status is being checked, OR;
- The OCSP response is signed by a separate OCSP Responder Certificate which is signed by the CA that issued the Certificate whose revocation status is being checked. In this case the signing certificate will contain an extension of type id-pkix- ocsp-nocheck, as defined by RFC6960.

All Sectigo?s OCSP responses are updated at least every 3.5 days and have a maximum expiration of 7 days. Relying parties must perform online revocation/status checks in accordance with section 4.9.6 of this CPS prior to relying on the Certificate.

### 4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

### 4.9.12 Special Requirements for Key Compromise

No stipulation.

### 4.9.13 Circumstances for Suspension

Not applicable.

### 4.9.14 Who can Request Suspension

Not applicable.

### 4.9.15 Procedure for Suspension Request

Not applicable.

### 4.9.16 Limits on Suspension Period

Not applicable.

## 4.10 Certificate Status Services

CRL and OCSP are Certificate status checking services available to relying parties.

### 4.10.1 Operational Characteristics

The OCSP conforms to RFC 5019. Revocation information for Ensured Certificates is available through 1 day after the expiry date of the Certificate, except for Code Signing Certificates where revocation information is provided past the expiry date.

### 4.10.2 Service Availability

Certificate status services are available 24/7.

### 4.10.3 Optional Features

No stipulation.

## 4.11 End of Subscription

A Subscriber's subscription service ends if:

- Ensured CA ceases operation,
- All of Subscriber's Certificates issued by Ensured are revoked without the renewal or rekey of the Certificates, or
- The Subscriber's Subscriber Agreement terminates or expires without renewal.

## 4.12 Key Escrow and Recovery

In general, Ensured does not provide key escrow or key backup services. In general, Ensured expects an Applicant to generate key-pairs in its own environment and to pass only the public key to Ensured for inclusion in the Certificates issued.

In certain enterprise scenarios, where specifically provided for by contract between Ensured and the Subscriber enterprise, Ensured provides key backup for Certificates to be used for document signing and provides key escrow for Certificates to be used for (typically email) encryption. In order to effectuate backup and escrow where contracted, Ensured generates the key-pairs for the relevant Certificates and passes the encrypted private key to the Subscriber along with the original delivery of the public Certificate.

### 4.12.1 Key Escrow and Recovery Policy and Practices

An escrowed private key can only be recovered after Ensured confirms the authority of the party requesting the private key. Private keys may only be recovered for lawful and legitimate purposes. Ensured recommends to its Certificate Manager users that they notify their customers and Subscribers that their private keys are escrowed, that they protect escrowed keys from unauthorized disclosure, and that they do not disclose or allow to be disclosed any escrowed keys or (escrowed) key-related information to a third party unless required by law. Certificate Manager users are required to revoke the Certificate associated with an escrowed private key prior to retrieving the escrowed key from Ensured.

Escrowed private keys are kept for three years after the corresponding Certificate's expiry prior to their destruction. Private keys are destroyed by deleting the key from the storage material immediately, and from all related back up material within a further 12-month period.

### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

# 5. Facility, management and operational controls

This section of the CPS outlines the security policy, physical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.
Ensured asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

## 5.1 Physical Controls

All sites operate under a security policy designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to CA related facilities.

### 5.1.1 Site Location and Construction

Ensured operates in Europe with separate operations and server operation sites. Physical barriers are used to segregate secure areas within buildings and are constructed so as to extend from real floor to real ceiling to prevent unauthorized entry. External walls of the sites are of solid construction.

### 5.1.2 Physical Access

Access to the Ensured systems within the secure facility is protected with locked cabinets and logical access controls. Security perimeters are clearly defined for all Ensured locations. All of Ensured's entrances and exits are secured or monitored by monitoring/control systems.

### 5.1.3 Power and Air Conditioning

Ensured secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating/air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

### 5.1.4 Water Exposures

Ensured has made reasonable efforts to ensure its secure facilities are protected from flood and water damage.

### 5.1.5 Fire Prevention and Protection

Ensured has made reasonable efforts to ensure its secure facilities are protected from fire and smoke damage (fire protection is made in compliance with local fire regulations). IT equipment is located to reduce the risk of damage or loss by fire. The level of protection from fire reflects the importance of the equipment.

### 5.1.6 Media Storage

Amongst other ways, Ensured protects media by storing it away from known or obvious fire/water hazards. Media is also backed up on-site and off-site.

### 5.1.7 Waste Disposal

Ensured disposes of waste in accordance with industry best practice. Ensured has procedures in place to dispose of all media types, including, but not limited to, paper documents, hardware, damaged devices, and read only optical devices. These procedures apply to all information classification levels, with the method of disposal dependent on the classification.

### 5.1.8 Off-Site Backup

Ensured backs up much of its information to a secure, off-site location that is sufficiently distant to escape damage from a disaster at the primary location. The frequency, retention, and extent of the backup is determined by management, taking into account the criticality and security requirements of the information. Backup of critical CA software is performed daily and is stored offsite. Backup of critical business information is performed daily and is stored offsite. Access to backup servers/media is restricted to authorized personnel only. Backup media is regularly tested through restoration to ensure it can be relied on in the event of a disaster. Backup servers/media is appropriately labeled according to the confidentiality of the information.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

Ensured ensures that all operators and administrators including Vetting Agents are acting in the capacity of a trusted role. Trusted roles relate to access to the Ensured's system(s), with functional permissions supplied on an individual basis. The management supplies permissions.
The list of personnel appointed to trusted roles is maintained and reviewed annually.

Trusted roles include but are not limited to the following:

- Developer: Responsible for development of CA systems.
- Security Officer: Overall responsibility for administering the implementation of the CA's security practices;
- Vetting Agents: Responsible for validating the authenticity and integrity of data to be included within Certificates via a suitable RA system and approve the generation/revocation/suspension of Certificates;
- Senior Vetting Agents: Vetting Agents role that is Authorized to perform subscriber key generation.
- System Operator: Responsible for operating the CA systems on a day to day basis. Authorized to perform system backup / recovery, viewing / maintenance of CA system archives and audit logs;
- Auditor: Authorized to view archives and audit logs of the CA Trustworthy Systems;

Trusted personnel must identify and authenticate themselves to the system before access is granted. Identification is via a username, with authentication requiring a password and digital Certificate.

#### 5.2.1.1 Number of Persons Required per Task

It is required that at least two CA Administrators take action to activate the CA private keys for signing, to generate new CA key-pairs, or to restore private keys. No single person has the capability to issue a PIV-I credential, or to issue an EV SSL, EV Code-signing or PDF-Signing Certificate.

#### 5.2.1.2 Identification and Authentication for Each Role

All personnel are required to authenticate themselves to CA systems before they may perform the duties of their role involving those systems.

## 5.3 Personnel Controls

Access to the secure parts of Ensured's facilities is limited using physical and logical access controls and is only accessible to appropriately authorized individuals filling trusted roles for which they are properly qualified and to which they have been appointed by management.

It is required that all personnel filling trusted roles are properly trained and have suitable experience before being permitted to adopt those roles.

### 5.3.1 Qualifications, Experience, and Clearance Requirements

Consistent with this CPS, Ensured follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

Administrator access is only granted on Ensured IT systems when there is a specific business need. New System Administrators are not given full administrator rights until they have demonstrated a detailed knowledge of Ensured IT systems & policies and that they have reached a suitable skill level satisfactory to the Server Systems Manager/Administrator or CEO. New administrators are closely monitored by the Server Systems Manager/Administrator for the first three months. Where systems allow, administrator access authentication is via a public/private key specifically issued for this purpose. This provides accountability of individual administrators.

### 5.3.2 Background Check Procedures

All trusted roles are background-checked before access is granted to Ensured's systems. These checks may include, but are not limited to, verification of the individual's identity using a government issued photo ID, credit history, employment history, education, character references, social security number, criminal background.

### 5.3.3 Training Requirements

Ensured provides suitable training to all staff before they take on a trusted role should they not already have the complete skill-set required for that role.

Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

### 5.3.4 Retraining Frequency and Requirements

Personnel in trusted roles have additional training when changes in industry standards or changes in Ensured's operations require it. Ensured provides refresher training and informational updates sufficient to ensure that trusted personnel retain the requisite degree of expertise.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulation

### 5.3.6 Sanctions for Unauthorized Actions

Any personnel who, knowingly or negligently, violate Ensured's security policies, exceed the use of their authority, use their authority outside the scope of their employment, or allow personnel under their supervision to do so may be liable to disciplinary action up to and including termination of employment. Should the unauthorized actions of any person reveal a failure or deficiency of training, sufficient training or retraining will be employed to rectify the shortcoming.

### 5.3.7 Independent Contractor Requirements

Assets are not taken off-site without prior written authorization. Persons taking assets off-site must have a legitimate business reason to do so, and must be able to provide adequate security to protect the asset during the time off-site. Once the independent contractor completes the work for which it was hired, or the independent contractor's employment is terminated, physical access rights assigned to that contractor are removed as soon as possible and within 24 hours from the time of termination.

### 5.3.8 Documentation Supplied to Personnel

The selection of documentation supplied to Ensured personnel is based on the role(s) they are to fill. Such documentation may include a copy of this CPS, the CABF EV Guidelines, and other technical and operational documentation necessary to maintain Ensured's CA operations.

## 5.4 Audit Logging Procedures

For audit purposes, electronic or manual logs of the following events for core functions are maintained.

### 5.4.1 Types of Events Recorded

An audit log is maintained of each movement of the removable media.

CA & Certificate Lifecycle Events:

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber Certificate life cycle management, including successful and unsuccessful Certificate applications, Certificate issuances, Certificate re-issuances and Certificate renewals
- Subscriber Certificate revocation requests, including revocation reason
- Subscriber changes of affiliation that would invalidate the validity of an existing Certificate
- CRL updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a private key

Security Related Events:

- System downtime, software crashes and hardware failures
- CA system actions performed by Ensured personnel, including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement

- Successful and unsuccessful Ensured PKI access attempts
- Secure CA facility visitor entry and exit

Certificate Application Information:

- The documentation and other related information presented by the Applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

### 5.4.2 Frequency of Processing Log

Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management.

### 5.4.3 Retention Period for Audit Log

When the removable media reaches the end of its life it is wiped by management or a third party secure data destruction facility and the Certificates of destruction are archived.

### 5.4.4 Protection of Audit Log

These media are only removed by staff on a visit to the data center, and when not in the data center are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.
Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction.

### 5.4.5 Audit Log Backup Procedures

All logs are backed up on removable media and the media held at a secure off-site location on a daily basis.

### 5.4.6 Audit Collection System (Internal vs. External)

Automatic audit collection processes run from system startup to system shutdown. The failure of an automated audit system which may adversely affect the integrity of the system or the confidentiality of the information protected by the system will lead to an evaluation whether a suspension of operations is required until the problem is remedied.

### 5.4.7 Notification to Event-Causing Subject

No stipulation.

### 5.4.8 Vulnerability Assessments

A vulnerability is a weakness in the organization or in an information system that might be exploited by a threat, with the possibility of causing harm to assets. In order to mitigate the risk or possibility of causing harm to assets, Ensured performs regular vulnerability assessment by taking a two-pronged approach. Ensured assesses vulnerabilities by (1) making an assessment of the threats to, impacts on, and the vulnerabilities of assets and the likelihood of their occurrence, and (2) by developing a process of selecting and implementing security controls in order to reduce the risks identified in the risk assessment to an acceptable level. Ensured routinely performs vulnerability assessments by identifying the vulnerability categories that face an asset. Some of the vulnerability categories that Ensured evaluates are technical, logical, human, physical, environmental, and operational.

Vulnerability scans are run by Ensured trusted staff on a weekly schedule. Additional scans are run following system updates, changes, or when deemed necessary.

Ensured employs external parties to perform regular annual vulnerability scans & penetration testing on our CA systems/infrastructure.

## 5.5 Records Archival

Ensured implements a backup standard for all business critical systems located at its data centers. Ensured retains records in electronic or in paper-based format in conformance with this subsection of the CPS.

### 5.5.1 Types of Records Archived

Ensured backs up both application and system data. Ensured may archive the following information:

- Audit data, as specified in section Audit Logging Proceduresof this CPS;
- Certificate application information;
- Documentation supporting a Certificate application;
- Certificate life-cycle information.

### 5.5.2 Retention Period for Archive

The retention period for archived information depends on the type of information, the information's level of confidentiality, and the type of system the information is stored on.

Records of Ensured digital Certificates and the associated documentation are retained for a term of not less than 7 years, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation. Copies of Certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that Ensured may see fit.

### 5.5.3 Protection of Archive

Records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction. Access to backup servers and/or backup media, backup utilities, or backup data, is restricted to authorized personnel only and adheres to a strict default deny policy.

### 5.5.4 Archive Backup Procedures

Administrators at each Ensured location are responsible for carrying out and maintaining backup activities. Ensured employs both scheduled and unscheduled backups. Scheduled backups are automated using approved backup tools. Scheduled backups are monitored using automated tools. Unscheduled backups occur before carrying out major changes to critical systems and are part of any change request that has a possible impact on data integrity or security. All backup media is labeled according to the information classification, which is based on the backup information stored on the media.

### 5.5.5 Requirements for Time-Stamping of Records

Records that are time-stamped include, but are not limited to, the following:

- Visitor entry,
- Visitor exit,
- Pidgin (Chat) within Ensured,
- Emails/tickets sent between Ensured and third parties,
- Subscriber Agreements,
- Certificate issuance, and
- Certificate revocation.

### 5.5.6 Archive Collection System (Internal or External)

Ensured's archive collection system is solely internal. As part of its internal collection procedures, Ensured may require Subscribers to submit appropriate documentation in support of a Certificate application.

## 5.6 Key Changeover

Towards the end of each private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public key Certificate is provided to Subscribers and relying parties through the delivery methods detailed below.

Ensured makes all its CA Root Certificates available in online repositories at www.ensured.com/repository.

Ensured provides the full Certificate chain to the Subscriber upon issuance and delivery of the Subscriber Certificate.

## 5.7 Compromise and Disaster Recovery

Organizations are regularly faced with events that may disrupt their normal business activities or may lead to loss of information and assets. These events may be the result of natural disasters, accidents, equipment failures, or deliberate

actions. This section details the procedures Ensured employs in the event of a compromise or disaster.

### 5.7.1 Incident and Compromise Handling Procedures

All incidents (including compromises), both suspected and actual, are reported to the appropriate authority for investigation. Depending on the nature and immediacy of the incident, the reporter of an incident is to document the incident details to help with incident assessment, investigation, solution, and future operational changes. Once the incident is reported, the appropriate authority makes an initial assessment. Next, a containment strategy is chosen and implemented. After an incident has been contained, eradication is necessary to eliminate components of the incident. During eradication, importance is given to identifying all affected areas so they can be remedied.

These procedures are in place to ensure that

- a consistent response to incidents happening to Ensured's assets,
- incidents are detected, reported, and logged, and
- clear roles and responsibilities are defined.

To maintain the integrity of its services Ensured has documented and implemented a business continuity plan. This plan defines and contains a formal incident management reporting process, incident response, and incident escalation procedures to ensure professional incident management and return to normal operations within a timely manner. Incidents are analyzed to identify possible causes and resolve weaknesses in Ensured's processes, software and infrastructure. The business continuity plan is reviewed as may be required, but at least once a year.

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

If Ensured determines that its computing resources, software, or data operations have been compromised, Ensured will investigate the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise, Ensured reserves the right to revoke affected Certificates, to revoke entity keys, to provide new public keys to users, and to re-certify subjects.

### 5.7.3 Entity Private Key Compromise Procedures

Due to the nature of the CA private keys, these are classified as highly critical to Ensured's business operations and continuity. If any of Ensured's private signing keys were compromised or were suspected of having been compromised, Ensured would make an assessment to determine the nature and extent of the compromise. In the most severe circumstances, all Certificates ever issued by the use of those keys would be revoked, notifying all owners of Certificates (by email) of that revocation, and offering to re-issue the Certificates to the customers with an alternative or new private signing key.

### 5.7.4 Business Continuity Capabilities after a Disaster

Ensured, in cooperation with Sectigo, operates a fully redundant CA system. In the event of a short- or long-term loss of an office location, operations at other offices will be increased. The backup CA is readily available in the event that the primary CA should cease operation. All of Ensured's critical computer equipment is housed in a co-location facility run by a commercial data-center, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. A fully redundant CA system is maintained by Sectigo for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Ensured will endeavor to minimize interruptions to its CA operations.

## 5.8 CA Termination

In case of termination of CA operations for any reason whatsoever, Ensured will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Ensured will take the following steps, where possible:

- Providing Subscribers of valid Certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoking all Certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking Subscriber's consent.
- Giving timely notice of revocation to each affected Subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Ensured's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

# 6. Technical security controls

This section addresses certain technological aspects of the Ensured and Sectigo infrastructure and PKI services.

Ensured and Sectigo are not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

The Ensured CA and Sectigo CA Infrastructures use trustworthy systems to provide Certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks provide a reasonable level of availability, reliability and correct operation and enforce a security policy.

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

Key pairs for End Entity Certificates issued pursuant to Adobe Approved Trust List requirements SHALL be generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2 using a key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6 of this CPS. Subscriber keys are generated during the ordering process by Senior Vetting Agents solely.

For Root CA Key Pairs created under this CPS Ensured has delegated its PKI infrastructure to Sectigo, and Sectigo has listed their CA Key Pair Generation in section 6.1.1 of their CPS which can be downloaded from https://sectigo.com/legal

### 6.1.2 Private Key Delivery to Subscriber

Ensured CAs that create Private Keys on behalf of Subscribers do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. For PDF signing Certificates, this is achieved through the use of a FIPS 140-2 level 3 protected token, containing Private Keys and Certificates encrypted by a temporary password created by the client, of at least twelve (12) characters. The physical token is then delivered by parcel service.

Ensured does not generate Private Keys for publicly trusted SSL Certificates.

Ensured ensures the integrity of any Public/Private Keys and the randomness of the key material through a suitable RNG or PRNG. If Ensured detects or suspects that the Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then Ensured revokes all Certificates that include the Public Key corresponding to the communicated Private Key.

### 6.1.3 Public Key Delivery to Certificate Issuer

PDF Signing Certificate requests are typically generated using the cryptographic service provider software required for the FIPS token, and processed manually by Ensured in the form of a PKCS#10 Certificate Signing Request (CSR). The private key remains on the cryptographic token, and cannot be exported to the Subscriber's hard drive.

### 6.1.4 CA Public Key Delivery to Relying Parties

Ensured's public keys are provided to Relying Parties in a few ways. One way is through the Repository. Additionally, public keys of Sectigo's and Ensured's Root CAs are embedded in browsers.

### 6.1.5 Key Sizes

Certificates must meet the following requirements for algorithm type and key size.

| RSA |
| --- |
| 2048 bit RSA key with SHA-256 hashing algorithm |

### 6.1.6 Public Key Parameters Generation and Quality Checking

Ensured generates the public key parameters. Ensured's CA keys are generated within a FIPS 140-2 certified HSM.

### 6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Ensured Certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on an Ensured Certificate the Relying Party must use X.509v3 compliant software. Ensured Certificates include key usage extension fields to specify the purposes for which the Certificate may be used and to technically limit the functionality of the Certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Ensured.

The possible key purposes identified by the X.509v3 standard are the following:

- Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity
- Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action (excluding Certificate or CRL signing, as in f) or g) below)
- Key encipherment, for enciphering keys or other security information, e.g. for key transport
- Data encipherment, for enciphering user data, but not keys or other security information as in c) above
- Key agreement, for use as a public key agreement key
- Key Certificate signing, for verifying a CA's signature on Certificates, used in CA Certificates only
- CRL signing, for verifying a CA's signature on CRLs
- Encipher only, public key agreement key for use only in enciphering data when used with key agreement
- Decipher only, public key agreement key for use only in deciphering data when used with key agreement

The appearance of a key usage in this section of the CPS does not indicate that Ensured does or will issue a Certificate with that key usage. To determine which key usages Sectigo will place on behalf of Ensured in issued subscriber Certificates, see Key Usage fields in Appendix C: Certificate Profiles.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

The Ensured CA Infrastructure uses trustworthy systems to provide Certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

Ensured strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber private key.

### 6.2.1 Cryptographic Module Standards and Controls

Ensured securely generates and protects its own private key(s), using a trustworthy system certified to FIPS 140-1, 140-2, or 140-3 level 3 or higher, and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The Ensured CA Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

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

The decryption key is split across m removable media and requires n of m to reconstruct the decryption key. Custodians in the form of two or more authorized Sectigo officers on request of Ensured are required to physically retrieve the removable media from the distributed physically secure locations.

### 6.2.3 Private Key Escrow

Ensured does not escrow Private Keys for any reason.

### 6.2.4 Private Key Backup

Generally, the Subscriber is solely responsible for protection of their private keys. Ensured does not backup Subscriber Private Keys. If required for business continuity Ensured backs up Root and Subordinate Private Keys under the same multi-person control as the original Private Key.

### 6.2.5 Private Key Archival

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration, as detailed in section Certificate Operational Periods and Key Pair Usage Periods of this CPS.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

### 6.2.7 Private Key Storage on Cryptographic Module

Private Keys are generated and stored inside Hardware Signing Modules (HSMs) which have been certified to at least FIPS 140 Level 3.

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment.

### 6.2.8 Method of Activating Private Key

Depending on the circumstances and the type of Certificate, a private key can be activated by Ensured, Subscriber, or other authorized personnel. Ensured's private keys are activated in accordance with the specifications of the cryptographic module. Subscriber must make all reasonable efforts to protect the integrity and confidentiality of its private key(s). Private keys remain active until deactivated.

### 6.2.9 Method of Deactivating Private Key

Depending on the circumstances and the type of Certificate, a private key can be deactivated by Ensured, Subscriber, or other authorized personnel.

### 6.2.10 Method of Destroying Private Key

Destroying a private key means the destruction of all active keys, both backed-up and stored. Destroying a private key may comprise of removing it from the HSM or removing it from the active backup set. Private keys are destroyed in accordance with FIPS PUB 140-2.

### 6.2.11 Cryptographic Module Rating

See section Cryptographic Module Standards and Controls of this CPS.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

When public keys are archived, they are archived according to procedures outlined in section Records Archival of this CPS.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificates are valid upon issuance by Ensured and acceptance by the Subscriber. Generally, the Certificate validity period will be from 12 to 39 months, however, Ensured reserves the right to offer validity periods outside of this standard validity period. Ensured verifies all information that is included in Certificates at time intervals of thirty-nine months or less.

The lifetime of Ensured's Root CA keys is set out in Table 6.3.2. Subordinate CA key lifetimes are either the same or shorter than those of the CA by which they are signed.

Ensured PKI Hierarchy
The following high-level representation of the Ensured PKI is used to illustrate the hierarchy utilised.

- Ensured Root CA (serial number = 4d 61 0d eb b8 83 00 b0 69 13 a7 55 a4 1b 4b 44, expiry = 2038-01-19)
- Ensured Document Signing CA (serial number = 7d c4 ca 1e ef cc d9 e5 ce fa 55 2b a8 97 88 7b, expiry = 2031-10-25)
- End Entity Digital Signature (serial number = x, expiry = 1/2/3 year from issuance)

Table 6.3.2:

| CA Number | Description | Usage | NotBefore | NotAfter | Key Size | Hash Algorithm | Serial |
|---|---|---|---|---|---|---|---|
| 1 | Ensured Root CA | Self-signed Root Certificate for Ensured | 23 Jul 2015 00:00:00 +0000 | 18 Jan 2038 23:59:59 +0000 | RSA 4096 bit | SHA384 | 4d 61 0d eb b8 83 00 b0 69 13 a7 55 a4 1b 4b 44 |
| 2 | Ensured Document Signing CA | Intermediate Certificate for PDF and Microsoft Document Signing | 25 Oct 2016 00:00:00 +0000 | 24 Oct 2031 23:59:59 +0000 | RSA 4096 bit | SHA384 | 7d c4 ca 1e ef cc d9 e5 ce fa 55 2b a8 97 88 7b |
| 3 | Ensured Root CA | Cross signed intermediate Certificate for the Ensured Root CA | 02 Nov 2016 00:00:00 +0000 | 21 Jan 2023 23:59:59 +0000 | RSA 4096 bit | SHA384 | 3e de ff 19 23 22 01 de 44 e8 a6 e8 4a 56 1f c9 |
| 4 | Ensured Timestamping CA | Intermediate Certificate for timestamping Certificates | 25 Oct 2016 00:00:00 +0000 | 24 Oct 2031 23:59:59 +0000 | RSA 4096 bit | SHA384 | 00 b5 f5 48 3f 45 b1 86 16 81 b8 71 a8 01 f9 d8 0b |

The Ensured Root CA key pair is protected in accordance with the AICPA/CICA WebTrust program compliant infrastructure and CPS.

## 6.4 Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys. Examples of activation data include, but are not limited to, PINs, passphrases, and portions of private keys used in a key-splitting regime.

### 6.4.1 Activation Data Generation and Installation

Activation data is generated in accordance with the specifications of the HSM. This hardware is certified by FIPS 140-2.

### 6.4.2 Activation Data Protection

The procedures used to protect activation data is dependent on whether the data is for smartcards or passwords. Smartcards are held by highly trusted personnel. Passwords and smartcards are subject to Sectigo?s Cryptographic Policy.

### 6.4.3 Other Aspects of Activation Data

No stipulation.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

Ensured ensures the integrity of its computer systems by implementing controls, such as

- Applying the same security controls to all systems co-located in the same zone with a Certificate System;
- Maintaining Root CA Systems in a high security zone and in an offline state or air-gapped from other networks;
- Maintaining and protecting Issuing Systems, Certificate Management Systems, and Security Support systems;
- Configuring Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in Ensured's operations and allowing only those that are approved by Ensured;
- Reviewing configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems on a weekly basis;
- Undergoing penetration tests on a periodic basis and after significant infrastructure or application upgrades;
- Granting administration access to Certificate Systems only to persons acting in trusted roles and requiring their accountability for the Certificate System's security; and
- Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

### 6.5.2 Computer Security Rating

No stipulation.

## 6.6 Lifecycle Technical Controls

### 6.6.1 System Development Controls

Ensured has formal policies in place to control, document and monitor the development of its CA systems. Development requests may only be raised by a restricted set of personnel. Development tasks are prioritized by the 'task requesters' within their area and then further prioritized by the development manager whilst considering the development task list in its entirety. The majority of changes are developed in-house by Ensured. In the event that Ensured 'buys-in' services (hardware and/or software), vendors are selected based on reputation and ability to supply products 'fit for purpose'.

On receipt of each development request a unique task ID and title are assigned that stay with the task throughout the development lifecycle.

The work-product of all development requests undergo peer review prior to release to the production environment to prevent malicious or erroneous software being loaded into the production environment.

Each task must be tested and signed off by the QA team before being deployed to the production environment. When issues are found by QA the QA team provide feedback to the developer to resolve the issues before development may proceed to release.

Development and QA team members do not have any access to the production environment. Access to these areas is strictly controlled.

Once the change has gone live to the production environment the task requester along with the testing team are advised and the change re-tested.

### 6.6.2 Security Management Controls

Ensured has tools and procedures to ensure that Ensured?s operational systems and applications retain their integrity and remain configured securely. These tools and procedures include checking the integrity of the application and security software.

### 6.6.3 Life Cycle Security Controls

No stipulation

## 6.7 Network Security Controls

Ensured, in cooperation with Sectigo, develops, implements, and maintains a comprehensive security program designed to protect its networks. In this security program, general protections for the network include:

- Segmenting Certificate Systems into networks or zones based on their functional, logical, and physical relationship;
- Applying the same security controls to all systems co-located in the same zone with a Certificate System;
- Maintaining Root CA Systems in a high security zone and in an offline state or air-gapped from other networks;
- Implementing and configuring Security Support Systems that protect systems and communications between systems inside secure zones and communications with non-Certificate Systems outside those zones;
- Configuring network boundary controls (firewalls, switches, routers, and gateways) with rules that support only the services, protocols, ports, and communications that Ensured has identified as necessary to its operations;
- For Certificate Systems, implementing detection and prevention controls to guard against viruses and malicious software; and
- Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

## 6.8 Time-Stamping

Ensured operates a trusted Time-Stamping Authority (TSA). The TSA provides an Authenticode time-stamping service which is intended for use in signing software when used in conjunction with an Ensured PDF-signing Certificate. No warranty is offered and no liability will be accepted for any use of the Ensured TSA which is made other than PDF files in conjunction with an Ensured PDF signing Certificate.

The Ensured TSA is hosted and maintained by Sectigo.

# 7. Certificate, CRL and OCSP profiles

Ensured uses the standard X.509, version 3 to construct digital Certificates for use within the Ensured PKI. X.509v3 allows a CA to add certain Certificate extensions to the basic Certificate structure. Ensured uses a number of Certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for digital Certificates.

## 7.1 Certificate Profile

Ensured incorporates by reference the following information in every digital Certificate it issues:

- Terms and conditions of the digital Certificate.
- Any other applicable Certificate policy as may be stated on an issued Ensured Certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customized elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a Certificate.
- Any other information that is indicated to be so in a field of a Certificate.

A Certificate profile contains fields as specified below:

- key usage extension field (CPS section Key Usage Purposes (as per X.509 v3 key usage field))
- extension criticality field (CPS section Processing Semantics for the Critical Certificate Policies Extension)
- basic constraints extension (CPS section Usage of Policy Constraints Extension)

Typical content of information published on an Ensured Certificate may include but is not limited to the following elements of information:

- Secure Server Certificates
    - Applicant's fully qualified domain name.
    - Applicant's organizational name.
    - Code of Applicant's country.
    - Organizational unit name, street address, city, state.
    - Issuing certification authority (Ensured).
    - Applicant's public key.
    - Ensured digital signature.
    - Type of algorithm.
    - Validity period of the digital Certificate.
    - Serial number of the digital Certificate.
- Secure Email Certificates and PDF Signing Certificates
    - Applicant's e-mail address.
    - Applicant's name.
    - Code of Applican's country.
    - Organization name, organizational unit name, street address, city, state.
    - Applicant's public key.
    - Issuing certification authority (Ensured).
    - Ensured digital signature.
    - Type of algorithm.
    - Validity period of the digital Certificate.
    - Serial number of the digital Certificate.

### 7.1.1 Version Number(s)

Certificate versions are denoted in Appendix C.

### 7.1.2 Certificate Extensions

Certificate extensions are exhibited in Appendix C.
Enhanced naming is the usage of an extended organization field in an X.509v3 Certificate. Information contained in the organizational unit field is also included in the Certificate Policy extension that Ensured may use.

### 7.1.3 Algorithm Object Identifiers

Ensured issues Certificates with algorithms indicated by the following OIDs:

From RFC5754:

```
sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsa
```

### 7.1.4 Name Forms

Name forms are as stipulated in Types of Names of this CPS.

#### 7.1.4.1 Issuer Information

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

#### 7.1.4.2 Subject Information ? Subscriber Certificates

Ensured represents that it followed the procedure set forth in its Certification Practice Statement to verify that, as of the Certificate?s issuance date, all of the Subject Information was accurate.

**Subject Distinguished Name Fields**

- commonName

If present in PDF signing Certificates, this field contains the Subject?s name and e-mail address.

- organizationName

If present in PDF signing Certificates, this field contains the Subject?s name and/or DBA as verified under Section 3.2.2.2 or 3.2.2.3. Ensured may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations; e.g., if the official record shows ?Company Name Incorporated?, we may use ?Company Name Inc.? or ?Company Name?.

Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, we may use the subject:organizationName field to convey a natural person Subject?s name or DBA.

- streetAddress

If present in PDF signing Certificates, this field contains the Subject?s street address information as verified under Section 3.2.2.2 or 3.2.2.3.

- localityName

If present in PDF signing Certificates, this field contains the Subject?s locality information as verified under Section 3.2.2.2 or 3.2.2.3. Where the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(h), the localityName field may contain the Subject?s locality and/or state or province information as verified under Section 3.2.2.2 or 3.2.2.3.

- stateOrProvinceName

If present in PDF signing Certificates, this field contains the Subject?s state or province information as verified under Section 3.2.2.2 or 3.2.2.3. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(h), the subject:stateOrProvinceName field may contain the full name of the Subject?s country information as verified under Section 3.2.2.2 or 3.2.2.3.

- postalCode

If present in PDF signing Certificates, this field contains the Subject?s zip or postal code information as verified under Section 3.2.2.2 or 3.2.2.3.

- countryName

If present in PDF signing Certificates, this field contains the Subject?s two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3. If a Country is not represented by an official ISO 3166-1 country code, Ensured will specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

- organizationalUnitName

Ensured implements processes that prevent an organizationalUnitName attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the we have verified this information in accordance with Section 3.2.2.2 or 3.2.2.3 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in under Section 3.2.2.2 or 3.2.2.3.

#### 7.1.4.3 Subject Information ? Root Certificates and Subordinate CA Certificates

Ensured represents that Sectigo followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate?s issuance date, all of the Subject Information was accurate.

**Subject Distinguished Name Fields**

- commonName

This field will be present and may be used as an identifier for the CA certificate. Across all CA Certificates issued by Ensured, each unique subject:commonName will be paired with only one CA keypair.

- organizationName

This field will be present and contains the Subject CA?s name or DBA as verified under Section 3.2.2.2. Ensured may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations; e.g., if the official record shows ?Company Name Incorporated?, we may use ?Company Name Inc.? or ?Company Name?.

- countryName

This field will be present and contains the Subject?s two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3.

### 7.1.5 Name Constraints

No stipulation.

### 7.1.6 Certificate Policy Object Identifier

Certificate policy OIDs are listed in Appendix C under the applicable Certificate.

### 7.1.7 Usage of Policy Constraints Extension

The Basic Constraints extension specifies whether the subject of the Certificate may act as a CA or only as an end-entity. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Ensured.

### 7.1.8 Policy Qualifiers Syntax and Semantics

Policy qualifiers are stipulated in the Certificates listed in Appendix C.

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The extension criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the Certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

## 7.2 CRL Profile

Ensured manages and makes publicly available directories of revoked Ensured Certificates using CRLs. These CRL's are maintained and issued by Sectigo. All Ensured CRLs issued by Sectigo are X.509v2 CRLs, in particular as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked Certificates at all times prior to relying on information featured in a Certificate. Ensured updates and publishes a new CRL every 24 hours or more frequently under special circumstances. The CRL for end entity Certificates can be accessed via the following URL: http://crl.ensuredca.com/EnsuredDocumentSigningCA_2.crl

| | |
|---|---|
| Version | See CPS 7.2.1. |
| Issuer Name | CountryName = [Root Certificate Country Name],<br><br>OrganizationName=[Root Certificate Organization],<br>CommonName=[Root Certificate Common Name]<br>[UTF8String encoding] |
| This Update | [Date of Issuance] |
| Next Update | [Date of Issuance + no more than 10 days] |
| Revoked Certificates | CRL Entries<br><br>Certificate Serial Number<br>[Certificate Serial Number]<br>Date and Time of Revocation<br>[Date and Time of Revocation] |

### 7.2.1 Version Number(s)

Ensured issues X.509 Version 2 CRLs.

### 7.2.2 CRL and CRL Entry Extensions

| Extension | Value |
|---|---|
| CRL Number | Never repeated monotonically increasing integer |
| Authority Key Identifier | Same as the authority key identifier listed in the Certificate. |
| Invalidity Date | Date in UTC format |
| Reason Code | Optional reason for revocation |

## 7.3 OCSP Profile

Certificate status information for Ensured's Certificates is published using Online Certificate Status Protocol (OCSP). The infrastructure for Ensured's OCSP are set up and maintained and owned by Sectigo. The OCSP responders are capable of providing a 'good' or 'revoked' status for all Certificates issued under the terms of this CPS. In the case of Code Signing Certificates only, the OCSP responders will continue to give a 'good' status for unrevoked Certificates even after their expiry - for at least 20 years from issuance. In the case of all other Certificate types the OCSP responders will give an 'unknown' response for expired Certificates.

The OCSP service for Ensured's Certificates can be reached at http://ocsp.ensuredca.com. Revocation information is made immediately available through the OCSP services. The OCSP responder and responses are available 24x7.

### 7.3.1 Version Number(s)

The OCSP responder for Ensured's Certificates conforms to RFC 6960 and 5019.

### 7.3.2 OCSP Extension

No stipulation

# 8. Compliance, audit and other assessments

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust for Certification Authorities ("WebTrust for CAs"), ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

A regular audit is performed by an independent external auditor to assess Ensured's compliancy with the AICPA/CICA WebTrust for CAs.

## 8.1 Frequency or Circumstances of Assessment

WebTrust for CAs audit: The audit mandates that the period during which a CA issues Certificates be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

## 8.2 Identity/Qualifications of Assessor

WebTrust for CAs audit: This audit is performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in a latest applicable version of WebTrust for Certification Authorities;
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

## 8.3 Assessor's Relationship to Assessed Entity

WebTrust for CAs audit: The auditor is independent of Ensured, and does not have a financial interest, business relationship, or course of dealing that would create a conflict of interest or create a significant bias (for or against) Ensured.

## 8.4 Topics Covered by Assessment

As per current version of WebTrust for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities ? SSL Baseline with Network Security which can be found at http://www.webtrust.org

## 8.5 Actions Taken as a Result of Deficiency

WebTrust for CAs audit: Either remediate or the auditor posts "qualified report." Auditor would report or document the deficiency, and notify Ensured of the findings. Depending on the nature and extent of the deficiency, Ensured would develop a plan to correct the deficiency, which could involve changing its policies or practices, or both. Ensured would then put its amended policies or practices into operation and require the auditors to verify that the deficiency is no longer present. Ensured would then decide whether to take any remedial action with regard to Certificates already issued.

## 8.6 Communication of Results

WebTrust for CAs audit: The audit requires that Ensured make the Audit Report available to the public. Ensured is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

## 8.7 Self-Audit

Ensured monitors its adherence to Certificate Policy, Certification Practice Statement and other external requirements specified in the "Acknowledgements" section and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected samples at least 3 percent of the Certificates issued.

# 9. Other business and legal matters

This part describes the legal representations, warranties and limitations associated with Ensured digital Certificates.

## 9.1 Fees

Ensured charges Subscriber fees for some of the Certificate services it offers, including issuance, renewal and reissues (in accordance with the Ensured Reissue Policy stated in Reissue Policy of this CPS). Such fees are detailed on the official Ensured website www.ensured.com.

Ensured retains its right to affect changes to such fees. Ensured partners, including Resellers will be suitably advised of price amendments as detailed in the relevant partner agreements.

### 9.1.1 Certificate Issuance or Renewal Fees

Ensured is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. In most circumstances, applicable Certificate fees will be delineated in the Subscriber Agreement between Ensured and Subscriber.

### 9.1.2 Certificate Access Fees

Ensured may charge a reasonable fee for access to its Certificate databases.

### 9.1.3 Revocation or Status Information Access Fees

Ensured does not charge fees for the revocation of a Certificate or for a Relying Party to check the validity status of an Ensured issued Certificate using CRLs.

### 9.1.4 Fees for Other Services

Ensured is entitled to charge a reasonable fee for checking the validity status of an Ensured issued Certificate using OCSP. Ensured is entitled to charge a reasonable fee for key recovery. Such fees are detailed on the official Ensured website www.ensured.com.

### 9.1.5 Refund Policy

Ensured offers a 30-day refund policy for SSL Certificates. During a 30-day period (beginning when a Certificate is first issued) the Subscriber may request a full refund for their SSL Certificate. Under such circumstances, the original Certificate may be revoked and a refund provided to the Applicant. Ensured is not obliged to refund a SSL Certificate after the 30-day reissue policy period has expired. Ensured does not refund Signing Certificates.

### 9.1.6 Reissue Policy

Ensured offers a free of charge reissue policy. If details other than just the public key require amendment, Ensured reserves the right to revalidate the application in accordance with the validation processes detailed within this CPS. If the reissue request does not pass the validation process, Ensured reserves the right to refuse the reissue application. Under such circumstances, the original Certificate may be revoked. A refund will be provided to the Applicant in case the refused reissue application is within 30 days of the original application.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

Ensured maintains professional Errors and Omissions Insurance.

### 9.2.2 Other Assets

No stipulation.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

Certificate Limited Warranty Plan: If Ensured was negligent in issuing a digital Certificate that resulted in a loss to a Relying Party, Relying Party may be eligible under Ensured's Certificate warranty to receive up to the Maximum Certificate Coverage per incident, subject to the Total Payment Limit shown in Table Insurance or Warranty Coverage for End-Entities below for all claims related to that digital Certificate. Except to the extent of willful misconduct, the liability of Ensured is limited to the negligent issuance of Certificates. The Maximum Certificate Coverage of Ensured to all Applicants, Subscribers and relying parties for each Certificate is set forth in Table Insurance or Warranty Coverage for End-Entities below. Under Ensured's warranty a covered person may only receive a payment in accordance with the Maximum Certificate Coverage set forth in Table Insurance or Warranty Coverage for End-Entities per online transaction for which the Covered Person claims there was a breach of the Ensured Warranty (each an "Incident"). If multiple Covered Persons are affiliated as to a common entity, then those multiple Covered Persons collectively are eligible to receive a maximum amount in accordance with the Maximum Certificate Coverage set forth in Table Insurance or Warranty Coverage for End-Entities per Incident. Any payments to Covered Persons shall be limited by the Total Payment Limit for any claims relating to that Digital Certificate. For example, if a Digital Certificate carries a Total Payment Limit of $10,000, then Covered Persons can receive payments in accordance with this warranty for up to the Maximum Certificate Coverage per Incident until a total of $10,000 has been paid in the aggregate for all claims by all parties related to that Digital Certificate. Upon renewal of any Digital Certificate, the total claims paid for such a Digital Certificate shall be reset to zero dollars.

Table Insurance or Warranty Coverage for End-Entities

| Ensured Certificate Type | Maximum Certificate Coverage | Total Payment Limit |
|---|---|---|
| Ensured Document Signing for AATL certificate (Adobe Approved Trust List) | 2500 USD | 10000 USD |
| Ensured Timestamping Certificate | 2500 USD | 10000 USD |

#### 9.2.3.1 Apportionment of claims

Damages exceeding the maximum warranty limit above for any given Certificate shall be apportioned first to the earliest claims to achieve final resolution. Ensured shall not pay more than the maximum warranty limit for each Certificate, regardless of the method of apportionment among claimants, or number of digital signatures, transactions, or claims related to a Certificate.

#### 9.2.3.2 Total amount for warranty exhausted

When the maximum limit allocated for warranty payments is exhausted, Ensured shall have no further obligation to refund any Beneficiary, unless required otherwise by applicable law.

## 9.3 Confidentiality of Business Information

Ensured observes applicable rules on the protection of personal data deemed by law or the Ensured privacy policy (see section Privacy Plan of this CPS) to be confidential.

### 9.3.1 Scope of Confidential Information

Ensured keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Subscriber Agreements.
- Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports, except for WebTrust audit reports that may be published at the discretion of Ensured.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Ensured infrastructure, Certificate management and enrolment services and data.

### 9.3.2 Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all Certificates issued by the Sectigo is public information and is published every 24 hours. Subscriber application data marked as ?Public? in the relevant Subscriber Agreement or Certificate request form that is submitted as part of a Certificate application is published within an issued Certificate. Such information is not within the scope of confidential information.

#### 9.3.3 Responsibility to Protect Confidential Information

All personnel in trusted positions handle all information in strict confidence. Personnel must comply with the requirements of the Dutch law on the protection of personal data.

#### 9.3.4 Publication of Certificate Revocation Data

Ensured reserves its right to publish a CRL as may be indicated.

### 9.4 Privacy of Personal Information

#### 9.4.1 Privacy Plan

Ensured has implemented a privacy policy, which complies with this CPS and the guidelines of the Autoriteit Persoonsgegevens

#### 9.4.2 Information Treated as Private

See Ensured CA Limited Privacy Policy. Additionally, personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in the Certificate and if the information is not public information.

#### 9.4.3 Information not Deemed Private

In addition to the information not deemed private in the Ensured CA Limited Privacy Policy, information made public in a Certificate, CRL, or OCSP is not deemed private.

#### 9.4.4 Responsibility to Protect Private Information

Ensured participants are expected to handle private information with care, and in compliance with local privacy laws in the relevant jurisdiction.

#### 9.4.5 Notice and Consent to use Private Information

Ensured will only use private information after obtaining consent or as required by applicable laws or regulations.

#### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Ensured reserves the right to disclose personal information if Ensured reasonably believes that

- disclosure is required by law or regulation, or
- disclosure is necessary in response to judicial, administrative, or other legal processes.

#### 9.4.7 Other Information Disclosure Circumstances

Ensured is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom Ensured owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

### 9.5 Intellectual Property Rights

Ensured or its partners or associates own all intellectual property rights associated with its databases, websites, Ensured digital Certificates and any other publication originating from Ensured including this CPS.

### 9.6 Representations and Warranties

#### 9.6.1 CA Representations and Warranties

Ensured makes to all Subscribers and relying parties certain representations regarding its public service, as described below. Ensured reserves its right to modify such representations as it sees fit or required by law.

Except as expressly stated in this CPS or in a separate agreement with Subscriber, to the extent specified in the relevant sections of the CPS, Ensured promises to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Ensured Repository and website for the operation of PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of Certificates that it may make publicly available.
- Issue digital Certificates in accordance with this CPS and fulfill its obligations presented herein.
- Publish accepted Certificates in accordance with this CPS.
- Provide support to Subscribers and relying parties as described in this CPS.
- Revoke Certificates according to this CPS.
- Provide for the expiration and renewal of Certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.
- Warrant the accuracy of information published on a Qualified Certificate issued pursuant to the requirements of the European Directive 99/93.
- Warrant that the signatory held the private key at the time of issuance of a Certificate issued pursuant to the requirements for Qualified Certificates as in the European Directive 99/93.

The Subscriber also acknowledges that Ensured has no further obligations under this CPS.

### 9.6.2 Subscriber Representations and Warranties

Subscribers represent and warrant that when submitting to Ensured and using a domain and distinguished name (and all other Certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Upon accepting a Certificate, the Subscriber represents to Ensured and to relying parties that at the time of acceptance and until further notice:

- Digital signatures created using the private key corresponding to the public key included in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorized person has ever had access to the Subscriber's private key.
- All representations made by the Subscriber to Ensured regarding the information contained in the Certificate are accurate and true.
- All information contained in the Certificate is accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber had notice of such information whilst the Subscriber shall act promptly to notify Ensured of any material inaccuracies in such information.
- The Certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use an Ensured Certificate only in conjunction with the entity named in the organization field of a digital Certificate (if applicable).
- The Subscriber retains control of her private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Subscriber is an end-user Subscriber and not a CA, and will not use the private key corresponding to any public key listed in the Certificate for purposes of signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and Ensured.
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of Ensured.
- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

In all cases and for all types of Ensured Certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Ensured of any such changes.

### 9.6.3 Relying Party Representations and Warranties

A party relying on an Ensured Certificate accepts that in order to reasonably rely on an Ensured Certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected Certificate; the Relying Party must have reasonably made the effort to acquire sufficient knowledge on using digital Certificates and PKI.
- Study the limitations to the usage of digital Certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using an Ensured digital Certificate.
- Read and agree with the terms of the Ensured CPS and Relying Party agreement.
- Verify an Ensured Certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or by checking the OCSP response.
- Trust an Ensured Certificate only if it is valid and has not been revoked or has expired.
- Rely on an Ensured Certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

## 9.7 Disclaimers of Warranties

### 9.7.1 Fitness for a Particular Purpose

Ensured disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law.

### 9.7.2 Other Warranties

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93 Ensured does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in Certificates or otherwise compiled, published, or disseminated by or on behalf of Ensured except as it may be stated in the relevant product description below in this CPS and in the Ensured insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in Ensured Personal Certificates class 1, free, trial or demo Certificates.
- In addition, shall not incur liability for representations of information contained in a Certificate except as it may be stated in the relevant product description in this CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although Ensured is responsible for the revocation of a Certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of Certificates issued by a third party (including an agent) unless specifically stated by Ensured.

Ensured assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. Ensured cannot warrant that such user software will support and enforce controls required by Ensured, whilst the user should seek appropriate advice.

## 9.8 Limitations of Liability

Ensured Certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the Certificate and disclaimers of warranty that may apply. Subscribers must agree to Ensured Terms & Conditions before signing-up for a Certificate. To communicate information Ensured may use:

- An organizational unit attribute.
- An Ensured standard resource qualifier to a Certificate policy.
- Proprietary or other vendors' registered extensions.

### 9.8.1 Damage and Loss Limitations

In no event (except for fraud or willful misconduct) will the aggregate liability of Ensured to all parties including without

any limitation a Subscriber, an Applicant, a recipient, or a Relying Party for all digital signatures and transactions related to such Certificate exceed the cumulative maximum liability for such a Certificate as stated in the Ensured insurance plan detailed section Insurance or Warranty Coverage for End-Entities of this CPS.

### 9.8.2 Exclusion of Certain Elements of Damages

In no event (except for fraud or willful misconduct) shall Ensured be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of Certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those due to reliance, on the information featured on a Certificate, on the verified information in a Certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the Applicant. Any liability that arises from the usage of a Certificate that has not been issued or used in conformance with this CPS.
- Any liability that arises from the usage of a Certificate that is not valid.
- Any liability that arises from usage of a Certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses.
- Any liability that arises from compromise of a Subscriber's private key.

Ensured does not limit or exclude liability for death or personal injury.

## 9.9 Indemnities

### 9.9.1 Indemnification by Subscriber

By accepting a Certificate, the Subscriber agrees to indemnify and hold Ensured, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that Ensured, and the above mentioned parties may incur, that are caused by the use or publication of a Certificate, and that arises from:

- Any false or misrepresented data supplied by the Subscriber or agent(s).
- Any failure of the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Ensured, or any person receiving or relying on the Certificate.
- Failure to protect the Subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

For Certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify Ensured, and its agents and contractors.

Although Ensured will provide all reasonable assistance, Certificate Subscribers shall defend, indemnify, and hold Ensured harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Ensured.

## 9.10 Terms and Termination

### 9.10.1 Terms

The term of this CPS, including amendments and addenda, begins upon publication to the Repository and remains in effect until replaced with a new CPS passed by the Ensured Certificate Policy Authority.

### 9.10.2 Termination

This CPS, including all amendments and addenda, remain in force until replaced by a newer version.

### 9.10.3 Effect of Termination and Survival

The following rights, responsibilities, and obligations survive the termination of this CPS for Certificates issued under this CPS:

- All unpaid fees incurred under section Feesof this CPS;
- All responsibilities and obligations related to confidential information, including those stated in section Confidentiality of Business Information of this CPS;
- All responsibilities and obligations to protect private information, including those stated in section Responsibility to Protect Private Information of this CPS;
- All representations and warranties, including those stated in section Representations and Warranties of this CPS;
- All warranties disclaimed in section Disclaimers of Warranties of this CPS for Certificates issued during the term of this CPS;
- All limitations of liability provided for in section Limitations of Liability of this CPS; and
- All indemnities provided for in section Indemnities of this CPS.

Upon termination of this CPS, all PKI participants are bound by the terms of this CPS for Certificates issued during the term of this CPS and for the remainder of the validity periods of such Certificates.

## 9.11 Individual Notices and Communications with Participants

Ensured accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Ensured, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

Ensured
Attention: Legal Practices
Rogier van der Weydestraat 2
1817 MJ Alkmaar
The Netherlands

Email: legal@ensured.com

This CPS, related agreements and Certificate policies referenced within this document are available online at www.ensured.com/repository.

## 9.12 Amendments

Upon the Ensured Certificate Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the Ensured repository (available at www.ensured.com/repository), with seven (7) days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

Revisions not denoted "significant" are those deemed by the Ensured Certificate Policy Authority to have minimal or no impact on Subscribers and relying parties using Certificates and CRLs issued by CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS.

Controls are in place to reasonably ensure that the Ensured CPS is not amended and published without the prior authorization of the Ensured Certificate Policy Authority.

### 9.12.1 Procedure for Amendment

An amendment to this CPS is made by the Ensured Certificate Policy Authority. The Ensured Certificate Policy Authority will approve amendments to this CPS, and Ensured will publish amendments in the Repository. Amendments can be an update, revision, or modification to this CPS document, and can be detailed in this CPS or in a separate document. Additionally, amendments supersede any designated or conflicting provisions of the amended version of the CPS.

## 9.13 Notification Mechanism and Period

Ensured provides notice of an amendment to the CPS by posting it to the Repository. Amendments become effective on the date provided in the document, when an amendment is written in a separate document, or on the date provided in this CPS, when written in this document.

Ensured does not guarantee or establish a notice and comment period.

#### 9.13.1 Circumstances Under Which OID Must be Changed

The Ensured Certificate Policy Authority has the sole authority to determine whether an amendment to the CPS requires an OID change.

## 9.14 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify Ensured of the dispute with a view to seek dispute resolution.

## 9.15 Governing Law, Interpretation, and Jurisdiction

### 9.15.1 Governing Law

This CPS is governed by, and construed in accordance with Dutch law. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of Ensured digital Certificates or other products and services. Dutch law applies in all Ensured commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to Ensured products and services where Ensured acts as a provider, supplier, beneficiary receiver or otherwise.

### 9.15.2 Interpretation

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services and products of Ensured as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

### 9.15.3 Jurisdiction

Each party, including Ensured partners, Subscribers and relying parties, irrevocably agrees that the courts of the Netherlands have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of Ensured PKI services.

## 9.16 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders, including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. In delivering its PKI services Ensured complies in all material respects with high-level international standards including those on Qualified Certificates pursuant to the European Directive 99/93 and the relevant law on electronic signatures and all other relevant legislation and regulation.

## 9.17 Miscellaneous Provisions

### 9.17.1 Entire Agreement

This agreement and all documents referred to herein constitutes the entire agreement between the parties, superseding all other agreements that may exist with respect to the subject matter. Section headings are for reference and convenience only and are not part of the interpretation of this agreement.

### 9.17.2 Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of

operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

### 9.17.3 Severability

If any term, provision, covenant, or restriction contained in this CPS, or the application thereof, is for any reason and to any extent held to be invalid, void, or unenforceable, (i) such provision shall be reformed to the minimum extent necessary to make it valid and enforceable as to affect the original intention of the parties, and (ii) the remainder of the terms, provisions, covenants, and restrictions of this CPS shall remain in full force and effect and shall in no way be affected, impaired or invalidated.

### 9.17.4 Enforcement (Attorneys' Fees and Waiver of Rights)

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision.

### 9.17.5 Force Majeure

Neither Ensured, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the forgoing shall be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of the Ensured CPS, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes include natural disasters or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Ensured is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labor materials, energy, utilities, components or machinery, acts of civil or military authorities.

### 9.17.6 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this CPS shall prevail and bind the Subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this CPS.
- Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

## 9.18 Other Provisions

### 9.18.1 Subscriber Liability to Relying Parties

Without limiting other Subscriber obligations stated in this CPS, Subscribers are liable for any misrepresentations they make in Certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the Certificate.

### 9.18.2 Duty to Monitor Agents

The Subscriber shall control and be responsible for the data that an agent supplies to Ensured. The Subscriber must promptly notify the issuer of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

### 9.18.3 Financial Limitations on Certificate Usage

Ensured Certificates may only be used in connection with data transfer and transactions completed using a credit card and having a Euro (?) value no greater than the max transaction value associated with the Certificate and detailed in the table in section Insurance or Warranty Coverage for End-Entities of this CPS.

### 9.18.4 Ownership

Certificates are the property of Ensured. Ensured gives permission to reproduce and distribute Certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Ensured reserves the right to revoke the Certificate at any time. Private and public keys are property of the Subscribers who rightfully issue and hold them. All secret shares (distributed elements) of the Ensured private key remain the property of Ensured.

### 9.18.5 Interference with Ensured Implementation

Subscribers, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of the PKI services including the key generation process, the public web site and the Ensured repositories except as explicitly permitted by this CPS or upon prior written approval of Ensured. Failure to comply with this as a Subscriber will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but that have not yet been paid under the agreement. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Ensured repository and any Certificate or Service provided by Ensured.

### 9.18.6 Choice of Cryptographic Method

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

### 9.18.7 Ensured Partnerships Limitations

Partners of Ensured shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Ensured products and services. Ensured partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Ensured repository and any Digital Certificate or Service provided by Ensured.

### 9.18.8 Subscriber Obligations

Unless otherwise stated in this CPS, Subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own private / public key pair to be used in association with the Certificate request submitted to Ensured.
- Ensure that the public key submitted to Ensured corresponds with the private key used.
- Ensure that the public key submitted to to Ensured is the correct one.
- Provide correct and accurate information in its communications with Ensured.
- Alert Ensured if at any stage whilst the Certificate is valid, any information originally submitted has changed since it had been submitted to Ensured.
- Generate a new, secure key pair to be used in association with a Certificate that it requests from Ensured.
- Read, understand and agree with all terms and conditions in this Ensured CPS and associated policies published in the Ensured Repository at www.ensured.com/repository.
- Refrain from tampering with an Ensured Certificate.
- Use Ensured Certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- Cease using an Ensured Certificate if any information in it becomes misleading obsolete or invalid.
- Cease using an Ensured Certificate if such Certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the Subscriber's private key corresponding to the public key in an Ensured issued Certificate to issue end-entity digital Certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in an Ensured Certificate.
- Request the revocation of a Certificate in case of an occurrence that materially affects the integrity of an Ensured Certificate.
- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their private keys.

# 10. Appendix A - Table of Acronyms

| Acronym | Full Name |
|---|---|
| AATL | Adobe Approved Trust List |
| AICPA | American Institute of Certified Public Accountants |
| BR | Baseline Requirements |
| CA | Certificate Authority |
| CA/B (or CAB) | Certificate Authority/Browser |
| CICA | Canadian Institute of Chartered Accountants |
| CPAC | Comodo Personal Authentication Certificate |
| CPS | Certification Practice Statement |
| CRL(s) | Certificate Revocation List(s) |
| CSR | Certificate Signing Request |
| CVC | Content Verification Certificate |
| DN | Distinguished Name |
| DSA | Digital Signature Algorithm |
| EPKI | Enterprise Public Key Infrastructure Manager |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| FIPS PUB | Federal Information Processing Standards Publication |
| FTP | File Transfer Protocol |
| HSM | Hardware Signing Module |
| HTTP | Hypertext Transfer Protocol |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ITU | International Telecommunication Union |
| ITU-T | ITU Telecommunication Standardization Sector |
| MDC | Multiple Domain Certificate |
| NIST | National Institute for Standards and Technology |
| OCSP | Online Certificate Status Protocol |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure (based on X.509 Digital Certificates) |
| PKCS | Public Key Cryptography Standard |
| RA(s) | Registration Authority(ies) |
| RFC | Request for Comments |
| SAN | Subject Alternate Name |
| SHA | Secure Hash Algorithm |
| SGC | Server Gated Cryptography |
| S/MIME | Secure/Multipurpose Internet Mail Extension(s) |
| SSL | Secure Sockets Layer |
| TLS | Transaction Layer Security |

| | |
|---|---|
| TSA | Time Stamping Authority |
| UTC | Coordinated Universal Time |
| URL | Uniform Resource Locator |

# 11. Appendix B - Table of Definitions

| Term | Definition |
|---|---|
| Applicant | Means the natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request. |
| Applicant Representative | Means a natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA. |
| Audit Report | Means a report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of the Baseline Requirements. |
| Basic Constraints | Means an extension that specifies whether the subject of the Certificate may act as a CA or only as an end-entity |
| Baseline Requirements | Means the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at http://www.cabforum.org. |
| Certificate | Means an electronic document that uses a digital signature to bind a public key and an entity. |
| Certificate Management System | Means a system used by Ensured to process, approve issuance of, or store Certificates or Certificate status information, including the database, database server, and storage. |
| Certificate Management | Means the functions that include but are not limited to the following: verification of the identity of an Applicant of a Certificate; authorizing the issuance of Certificates; issuance of Certificates; revocation of Certificates; listing of Certificates; distributing Certificates; publishing Certificates; storing Certificates; storing private keys; escrowing private keys; generating, issuing, decommissioning, and destruction of key pairs; retrieving Certificates in accordance with their particular intended use; and verification of the domain of an Applicant of a Certificate. |
| Certificate Manager | Means the software issued by Ensured and used by Subscribers to download Certificates. |
| Certificate Policy | Means a statement of the issuer that corresponds to the prescribed usage of a digital Certificate within an issuance context. |
| Certificate Systems | Means the system used by Ensured or a delegated third party in providing identity verification, registration and enrollment, Certificate approval, issuance, validity status, support, and other PKI-related services. |
| Ensured Certificate Policy Authority (XPA) | Means the entity charged with the Certificate Policy. |
| Front End/Internal Support System | Means a system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server. |
| Grace Period | Means the period during which the Subscriber must make a revocation request. |
| Issuing System | Means a system used to sign Certificates or validity status information. |
| Legal Entity | Means an association, corporation, partnership, proprietorship, trust, government entity, or other entity with legal standing in a country's legal system. |
| Reliable Method of Communication | Means a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative. |
| Relying Party | Means an entity that relies upon the information contained within the Certificate. |
| Relying Party Agreement | Means an agreement between Ensured and a Relying Party that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at www.ensured.com/repository. |
| Repository | Means Ensured's repository, available at www.ensured.com/respository. |
| Root CA System | Means a system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate. |
| Security Support System | Means a system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and anti-virus. |

| | |
|---|---|
| Subscriber | Means is an entity that has been issued a Certificate. |
| Subscriber Agreement | Means an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the digital Certificate product type as presented during the product online order process and is available for reference at www.ensured.com/repository. |
| WebTrust for Certification Authorities | Means the current program for CAs located at http://www.webtrust.org/homepage-documents/item27839.aspx. |
| X.509 | Means the ITU-T standard for Certificates and their corresponding authentication framework |

# 12. Appendix C - Certificate Profile

Repository: https://www.ensured.com/repository/

```
OCSP: ocsp.ensuredca.com
CRL: crl.ensuredca.com/EnsuredDocumentSigningCA_2.crl
CA Issuer: crt.ensuredca.com/EnsuredDocumentSigningCA_2.crt
```

### 12.0.1 General

```
O = Ensured B.V.
L = Heerhugowaard
ST = Noord-Holland
C = NL
```

### 12.0.1 Root

```
CN = Ensured Root CA
Signature Hash Algorithm = SHA-384
Key Size = 4096
```

### 12.0.1 Issuing CA

```
CN = Ensured Document Signing CA
Signature Hash Algorithm = SHA-384
Key Size = 4096
```

### 12.0.1 TimeStamping Service

```
CN = Ensured TimeStamping Service
RFC 3161 timestamps
```

| Field | Attribute | Value |
|---|---|---|
| Version | v3 | |
| Serial Number | [Automatically generated unique number] | |
| Signature Algorithm | SHA256RSA | |
| Signature Hash Algorithm | SHA-256 | |
| Issuer | CN | Ensured Document Signing CA |
| | O | Ensured B.V. |
| | L | Heerhugowaard |
| | S | Noord-Holland |
| | C | NL |
| Validity | 12 - 39 Months | |
| Subject | CN | Common Name |
| | OU | Department |
| | O | Company Name |
| | E | Email address |
| | L | City |
| | S | State |
| | C | Country Code |
| Authority Key Identifier | KeyID | [Key-ID of Issuer Certificate] |
| KeyUsage (critical) | Digital Signature, Non-Repudiation | |

| | | |
|---|---|---|
| Extended Key Usage | PDF Signature (1.2.840.113583.1.1.5)<br>Microsoft Document Signing (1.3.6.1.4.1.311.10.3.12) | |
| basicConstraints | Subject Type | End Entity |
| Path Length Contraint | None | |
| Certificate Policies | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.44710.2.1<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier: https://www.ensured.com/repository | |
| Authority Information Access | [1]Authority Info Access<br>Access Method = id-ad-caIssuers (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://crt.ensuredca.com/EnsuredDocumentSigningCA_2.crt<br>[2]Authority Info Access<br>Access Method = id-ad-ocsp (1.3.6.1.5.5.7.48.1)<br>URL = http://ocsp.ensuredca.com | |
| CRL Distribution Policies | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://crl.ensuredca.com/EnsuredDocumentSigningCA_2.crl | |
| subjectAltName | Email address | |
| Thumbprint Algorithm | SHA1 | |
| Thumbprint | | |
| Subject Key Identifier | | |
| 1.2.840.113583.1.1.9.1 | | timestamping.ensuredca.com |

# 13. Appendix D - Certificate Types

The different Certificate types have differing intended usages and differing policies as described below.

At this time there are no different certificate types present.

# 14. Appendix E - Changelog

This document is approved for publication on September 5, 2019 by the Ensured Policy Authority (EPA). The following revisions were made by the original document.

| Date | Changes | Version | Author |
|---|---|---|---|
| 08-05-2014 | First draft | 1.0.1 | Paul Veening |
| 01-08-2014 | Updates after review | 1.0.2 | Paul Veening |
| 21-11-2014 | Converted to Ensured and updates | 1.0.3 | Paul Veening |
| 25-03-2015 | Updates after audit | 1.0.4 | Martine Heemstra |
| 15-12-2015 | Clarified division of Ensured's and Sectigo's responsibilities and tasks. | 1.0.5 | Paul Veening |
| 14-11-2016 | Updated CA certificates serial number and expire date to productions values | 1.0.6 | Jacco Rens |
| 05-04-2018 | Updated office address | 1.0.7 | Jacco Rens |
| 12-02-2019 | Updated root lifespan description, updated Trusted role description | 1.0.8 | Jacco Rens |
| 12-02-2019 | Updated Subscriber key generation, updated Subscriber key delivery | 1.0.8 | Jacco Rens |
| 19-08-2019 | Updated Comodo brand name to Sectigo | 1.0.9 | Eric Kramer |
| 04-09-2019 | Review of the document and alignment with Sectigo CPS | 1.1.0 | Eric Kramer |
| 09-03-2020 | Alignment with IETF RFC 3647, removal of SSL/TLS related items | 1.2.0 | Jacco Rens |
| 18-08-2020 | Updated document repository, added Other Participants | 1.2.1 | Jacco Rens |