



NOSICA SSL

Certificate Policy/ Certification Practice
Statement

Version 1.0



nosi
we believe in...

Table of contents

1. Introduction	15
1.1 Overview.....	15
1.2 DOCUMENT NAME AND IDENTIFICATION	15
1.2.1 Revisions.....	16
1.3 PKI PARTICIPANTS	16
1.3.1 CERTIFICATION AUTHORITIES (CA).....	16
1.3.2 REGISTRATION AUTHORITIES.....	17
1.3.3 SUBSCRIBERS	18
1.3.4 RELYING PARTIES.....	18
1.3.5 CERTIFICATE MANAGERS	18
1.3.6 OTHER PARTICIPANTS	19
1.4 CERTIFICATE USAGE	19
1.4.1 APPROPRIATE CERTIFICATE USES	19
1.4.2 PROHIBITED CERTIFICATE USES	19
1.5 Policy Administration.....	20
1.5.1 Organization Administering the Document	20
1.5.2 Contact Person	20
1.5.3 Person Determining CP/CPS suitability for the policy	21
1.5.4 CP/CPS Approval procedure.....	21
1.6 Definitions and Acronyms	21
1.6.1 Definitions	21
1.6.2 Acronyms	34
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	36

2.1. Repositories	36
2.2 PUBLICATION OF CERTIFICATION INFORMATION	36
2.3 TIME OR FREQUENCY OF PUBLICATION	37
2.4 ACCESS CONTROLS ON REPOSITORIES	37
3. IDENTIFICATION AND AUTHENTICATION.....	37
3.1 NAMING	37
3.1.1. TYPES OF NAMES.....	37
3.1.2. NEED FOR NAMES TO BE MEANINGFUL	38
3.1.3. ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS.....	38
3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS	38
3.1.5. UNIQUENESS OF NAMES.....	38
3.1.6. RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS	39
3.2 INITIAL IDENTITY VALIDATION.....	39
3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY	39
3.2.2. AUTHENTICATION OF ORGANIZATION AND DOMAIN IDENTITY	39
3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY	50
3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION	51
3.2.5. VALIDATION OF AUTHORITY	51
3.2.6 CRITERIA FOR INTEROPERATION.....	52
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	52
3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY	52
3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION.....	52
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	52
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	53

4.1.	CERTIFICATE APPLICATION.....	53
4.1.1	WHO CAN SUBMIT A CERTIFICATE APPLICATION	53
4.1.2	ENROLLMENT PROCESS AND RESPONSIBILITIES	53
4.2.	CERTIFICATE APPLICATION PROCESSING	55
4.2.1	PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS...	55
4.2.2	APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS	56
4.2.3	TIME TO PROCESS CERTIFICATE APPLICATIONS.....	57
4.2.4	CERTIFICATE AUTHORITY AUTHORISATION (CAA) Error! Bookmark not defined.	
4.3	CERTIFICATE ISSUANCE	57
4.3.1	CA ACTIONS DURING CERTIFICATE ISSUANCE	57
4.3.2	NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE.....	58
4.4	CERTIFICATE ACCEPTANCE.....	59
4.4.1	CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE	59
4.4.2	PUBLICATION OF THE CERTIFICATE BY THE CA.....	59
4.4.3	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES.....	59
4.5	KEY PAIR AND CERTIFICATE USAGE.....	59
4.5.1	SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE	59
4.5.2	RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE	60
4.6	CERTIFICATE RENEWAL	60
4.6.1	CIRCUMSTANCES FOR CERTIFICATE RENEWAL	60
4.6.2	WHO MAY REQUEST RENEWAL	60
4.6.3	PROCESSING CERTIFICATE RENEWAL REQUESTS	61
4.6.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	61

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE	61
4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA	61
4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	61
4.7 CERTIFICATE RE-KEY	61
4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY	61
4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY	61
4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS	61
4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	61
4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE	62
4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA	62
4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	62
4.8 CERTIFICATE MODIFICATION	62
4.8.1 CIRCUMSTANCES FOR CERTIFICATE MODIFICATION	62
4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION	62
4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS	62
4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	62
4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE	62
4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA	62
4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	63
4.9 CERTIFICATE REVOCATION AND SUSPENSION	63
4.9.1 CIRCUMSTANCES FOR REVOCATION	63

4.9.2 WHO CAN REQUEST REVOCATION	65
4.9.3 PROCEDURE FOR REVOCATION REQUEST	65
4.9.4 REVOCATION REQUEST GRACE PERIOD	66
4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST	66
4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES.....	67
4.9.7 CRL ISSUANCE FREQUENCY	67
4.9.8 MAXIMUM LATENCY FOR CRLS.....	68
4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY	68
4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS.....	69
4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE.....	69
4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE	70
4.9.13 CIRCUMSTANCES FOR SUSPENSION	70
4.9.14 WHO CAN REQUEST SUSPENSION	70
4.9.15 PROCEDURE FOR SUSPENSION REQUEST	70
4.9.16 LIMITS ON SUSPENSION PERIOD	70
4.10 CERTIFICATE STATUS SERVICES	70
4.10.1 OPERATIONAL CHARACTERISTICS	70
4.10.2 SERVICE AVAILABILITY	71
4.10.3 OPTIONAL FEATURES	71
4.11 END OF SUBSCRIPTION.....	71
4.12 KEY ESCROW AND RECOVERY	71
4.12.1. KEY ESCROW AND RECOVERY POLICY AND PRACTICES	71
4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES.....	72
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	72



5.1.	PHYSICAL CONTROLS	73
5.1.1	SITE LOCATION AND CONSTRUCTION	73
5.1.2	PHYSICAL ACCESS	74
5.1.3	POWER AND AIR CONDITIONING	75
5.1.4	WATER EXPOSURES	75
5.1.5	FIRE PREVENTION AND PROTECTION	75
5.1.6	MEDIA STORAGE	75
5.1.7	WASTE DISPOSAL.....	76
5.1.8	OFF-SITE BACKUP	76
5.2.	PROCEDURAL CONTROLS	76
5.2.1	TRUSTED ROLES	76
5.2.2	NUMBER OF PERSONS REQUIRED PER TASK.....	80
5.2.3	IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE.....	80
5.2.4	ROLES REQUIRING SEPARATION OF DUTIES	81
5.3.	PERSONNEL CONTROLS	81
5.3.1	QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS..	81
5.3.2	BACKGROUND CHECK PROCEDURES.....	81
5.3.3	TRAINING REQUIREMENTS	82
5.3.4	RETRAINING FREQUENCY AND REQUIREMENTS.....	82
5.3.5	JOB ROTATION FREQUENCY AND SEQUENCE	83
5.3.6	SANCTIONS FOR UNAUTHORIZED ACTIONS.....	83
5.3.7	INDEPENDENT CONTRACTOR REQUIREMENTS.....	83
5.3.8	DOCUMENTATION SUPPLIED TO PERSONNEL	83
5.4.	AUDIT LOGGING PROCEDURES	84
5.4.1	TYPES OF EVENTS RECORDED.....	84

5.4.2 FREQUENCY OF PROCESSING LOG	86
5.4.3 RETENTION PERIOD FOR AUDIT LOG	86
5.4.4 PROTECTION OF AUDIT LOG.....	87
5.4.5 AUDIT LOG BACKUP PROCEDURES	87
5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL).....	87
5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT	87
5.4.8 VULNERABILITY ASSESSMENTS.....	88
5.5. RECORDS ARCHIVAL.....	89
5.5.1 TYPES OF RECORDS ARCHIVED	89
5.5.2 RETENTION PERIOD FOR ARCHIVE	89
5.5.3 PROTECTION OF ARCHIVE	90
5.5.4 ARCHIVE BACKUP PROCEDURES.....	90
5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS	90
5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL).....	90
5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION	90
5.6. KEY CHANGEOVER	91
5.7. COMPROMISE AND DISASTER RECOVERY	91
5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES	91
5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED	92
5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES.....	93
5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER	94
5.7.5 MISS-ISSUANCE HANDLING PROCEDURES	94
5.8. CA OR RA TERMINATION.....	95
6. TECHNICAL SECURITY CONTROLS	96

6.1.	KEY PAIR GENERATION AND INSTALLATION	96
6.1.1	KEY PAIR GENERATION.....	96
6.1.1.1	CA KEY PAIR GENERATION.....	96
6.1.2	PRIVATE KEY DELIVERY TO SUBSCRIBER.....	98
6.1.3	PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER	98
6.1.4	CA PUBLIC KEY DELIVERY TO RELYING PARTIES.....	99
6.1.5	KEY SIZES.....	99
6.1.6	PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING .	100
6.1.7	KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD).....	100
6.2.	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	100
6.2.1.	CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS	101
6.2.2	PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL.....	101
6.2.3	PRIVATE KEY ESCROW	101
6.2.4	PRIVATE KEY BACKUP	102
6.2.5	PRIVATE KEY ARCHIVAL.....	102
6.2.6	PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE	102
6.2.7	PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE	102
6.2.8	ACTIVATING PRIVATE KEY	102
6.2.9	DEACTIVATING PRIVATE KEY	103
6.2.10	DESTROYING PRIVATE KEY.....	103
6.2.11	CRYPTOGRAPHIC MODULE RATING.....	103
6.3.	OTHER ASPECTS OF KEY PAIR MANAGEMENT	103
6.3.1	PUBLIC KEY ARCHIVAL.....	103

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS	103
6.4. ACTIVATION DATA	104
6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION	104
6.4.2 ACTIVATION DATA PROTECTION	104
6.4.3 OTHER ASPECTS OF ACTIVATION DATA	104
6.5. COMPUTER SECURITY CONTROLS.....	105
6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS	105
6.5.2 COMPUTER SECURITY RATING	105
6.6. LIFE CYCLE TECHNICAL CONTROLS	106
6.6.1 SYSTEM DEVELOPMENT CONTROLS.....	106
6.6.2 SECURITY MANAGEMENT CONTROLS.....	107
6.6.3 LIFE CYCLE SECURITY CONTROLS	107
6.7. NETWORK SECURITY CONTROLS.....	108
6.8. TIME-STAMPING.....	109
7. CERTIFICATE, CRL, AND OCSP PROFILES.....	109
7.1. CERTIFICATE PROFILE	109
7.1.1 VERSION NUMBER(S).....	109
7.1.2 CERTIFICATE EXTENSIONS	109
7.1.3 ALGORITHM OBJECT IDENTIFIERS.....	134
7.1.4 NAME FORMS.....	135
7.1.5 NAME CONSTRAINTS	140
7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER	140
7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION	140
7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS.....	140

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION	140
7.2. CRL PROFILE.....	141
7.2.1 VERSION NUMBER(S).....	142
7.2.2 CRL AND CRL ENTRY EXTENSIONS.....	142
7.3. OCSP PROFILE	147
7.3.1 Version Number	147
7.3.2 OCSP Extensions	147
8. COMPLIANCE AUDIT AND OTHER ASSEMENTS	148
8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	148
8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR.....	148
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY.....	149
8.4. TOPICS COVERED BY ASSESSMENT	149
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY	150
8.6. COMMUNICATION OF RESULTS	150
8.7. SELF-AUDITS.....	151
9. OTHER BUSINESS AND LEGAL MATTERS.....	152
9.1 FEES	152
9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES.....	152
9.1.2 CERTIFICATE ACCESS FEES	152
9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES	152
9.1.4 FEES FOR OTHER SERVICES.....	152
9.1.5 REFUND POLICY	152
9.2. FINANCIAL RESPONSIBILITY	153
9.2.1 INSURANCE COVERAGE.....	153

9.2.2 OTHER ASSETS.....	153
9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES.....	153
9.3. CONFIDENTIALITY OF BUSINESS INFORMATION	153
9.3.1 SCOPE OF CONFIDENTIAL INFORMATION.....	153
9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION	154
9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION	154
9.4. PRIVACY OF PERSONAL INFORMATION	154
9.4.1 PRIVACY PLAN	154
9.4.2 INFORMATION TREATED AS PRIVATE.....	154
9.4.3 INFORMATION NOT DEEMED PRIVATE.....	155
9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION	155
9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION	155
9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS	155
9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES.....	155
9.5. INTELLECTUAL PROPERTY RIGHTS.....	155
9.6. REPRESENTATIONS AND WARRANTIES	156
9.6.1 CA REPRESENTATIONS AND WARRANTIES.....	156
9.6.2 RA REPRESENTATIONS AND WARRANTIES.....	157
9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES	157
9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES	159
9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS...	160
9.7. DISCLAIMERS OF WARRANTIES	160
9.8. LIMITATIONS OF LIABILITY.....	160
9.9. INDEMNITIES.....	161

9.9.1 INDEMNIFICATION BY NOSICA SSL.....	161
9.9.2 INDEMNIFICATION BY SUBSCRIBERS	162
9.9.3 INDEMNIFICATION BY RELYING PARTIES	162
9.10. TERM AND TERMINATION.....	162
9.10.1 TERM.....	162
9.10.2 TERMINATION.....	163
9.10.3 EFFECT OF TERMINATION AND SURVIVAL	163
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS	163
9.12. AMENDMENTS.....	163
9.12.1 PROCEDURE FOR AMENDMENT	163
9.12.2 NOTIFICATION MECHANISM AND PERIOD	163
9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED	163
9.13. DISPUTE RESOLUTION PROVISIONS	164
9.14. GOVERNING LAW.....	164
9.15. COMPLIANCE WITH APPLICABLE LAW	164
9.16. MISCELLANEOUS PROVISIONS.....	164
9.16.1 ENTIRE AGREEMENT.....	164
9.16.2 ASSIGNMENT.....	165
9.16.3 SEVERABILITY.....	165
9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS).....	166
9.16.5 FORCE MAJEURE	166
9.17. OTHER PROVISIONS.....	166
APPENDIX A: NOSICA SSL SUBSCRIBER CERTIFICATE PROFILE	Error! Bookmark not defined.
APPENDIX B: NOSICA SSL PKI END-ENTITY PROFILE	167



APPENDIX C: PROFILE OF THE CRL OF NOSICA SSL	172
APPENDIX D: OCSP RESPONDER CERTIFICATE PROFILE	173

1. INTRODUCTION

1.1 OVERVIEW

The NOSICA SSL is a Certificate Authority (CA) owned by NOSI, EPE. Referred as Certificate Policy and Certification Practice Statement (CP/CPS), this document has been prepared in compliance with the guide book of "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" for the purpose of describing how NOSICA SSL executes its operations during providing OV SSL (Organization Validated SSL) and DV SSL (Domain Validated SSL).

NOSICA SSL conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at <http://www.cabforum.org>. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

This CP/CPS document describes the execution of the services in regard to accepting Certificate applications, Certificate issuance and management, and Certificate revocation procedures in compliance with administrative, technical and legal requirements.

This CP/CPS also determines practice responsibilities and obligations of NOSICA SSL, applicants, subscribers and relying parties that use or rely on Certificates issued by NOSICA SSL.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP/CPS is divided into nine parts that cover the security controls and practices and procedures for Certificate services operated by NOSICA SSL. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation" along with a brief explanation of the reason.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the CP/CPS followed by NOSICA SSL while providing SSL certification services and was approved for publication by the NOSICA SSL Board of Directors. This CP/CPS document is disclosed to the public at <https://pki.nosi.cv/repositorio>.

NOSICA SSL organizes its OID for the various documents described in this CPS as follows:

Category	OID	Description
TLS	2.16.132.1.3.2.6	NOSICA SSL CPS
	2.16.132.1.2.2.6	NOSICA SSL CP

1.2.1 REVISIONS

Revisions of this document have been made as follows:

Version	Date	Comment	Changes
1.0	January, 18 2025	Initial Version	The whole document

1.3 PKI PARTICIPANTS

PKI Participants defined within the scope of this document are the parties bearing relevant rights and obligations within SSL certification services of NOSICA SSL. These parties are defined as CA, Registration Authority, Subscribers, Certificate Managers and Relying Parties.

1.3.1 CERTIFICATION AUTHORITIES (CA)

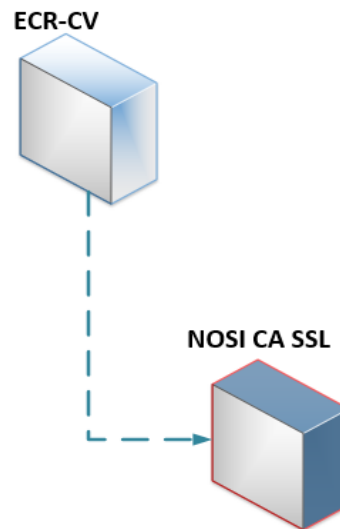
NOSICA SSL provides SSL certification services in accordance with this CP/CPS. As a CA, NOSICA SSL performs functions associated with Public Key operations, including receiving Certificate requests, issuing, and revoking SSL Certificates, and maintaining, issuing, and publishing CRLs and OCSP responses.

The NOSICA SSL PKI consists of a two-level CA hierarchy:

- ECRCV SSL root: signing all NOSICA SSL issuing CAs and kept offline. This CA is operated by the Multisectoral Regulatory Agency of the Economy - ARME, an entity that is part of the Government of Cape Verde. This CPS does not cover the operations of ECRCV.

- NOSICA SSL: This issuing CA is restricted to issue SSL certificates.

Certificate profiles issued by NOSICA SSL are detailed in Appendix A.



1.3.2 REGISTRATION AUTHORITIES

NOSICA SSL does not delegate the execution of Section 3.2 requirement to a Delegated Third Party. NOSICA SSL operates an internal Registration Authority located in the same infrastructure as its CA offerings, referred to in this document as NOSICA SSL RA, where all registration procedures are directly executed by NOSICA SSL personnel as described in Section 3.2.

NOSICA SSL personnel involved in the issuance of SSL certificates must meet and follow the requirements set out in Sections 4.2 and 5.3.

NOSICA SSL RA manages and performs the following roles and responsibilities:

- Identifying and authenticating Applicants for Certificates;
- Accepting, evaluating, approving or rejecting the registration of Certificate applications;

- Using authorized documents or sources of information to evaluate and authenticate an Applicant's application;
- Initiating the process to revoke a Certificate from the NOSICA SSL CA;
- Archiving of the registration files (electronic and / or paper).

1.3.3 SUBSCRIBERS

Subscribers are legal entities who apply for SSL Certificates from NOSICA SSL and agree to be bound by the relevant Subscriber Agreement. In this document, a Subscriber who has registered, but not yet received, a Certificate is referred to as an Applicant.

In some situations, NOSICA SSL acts as an Applicant or Subscriber, for instance, when it generates and protects a Private Key, requests a Certificate, demonstrates control of a Domain, or obtains a Certificate for its own use.

1.3.4 RELYING PARTIES

A Relying party is any natural person or legal entity that relies on a Valid SSL Certificate issued by NOSICA SSL. Relying Parties are responsible for verifying the validity of the Certificates.

To verify the validity of a Certificate, Relying Parties can refer to the CRL or OCSP response. The locations of the CRL distribution point and OCSP responder are detailed within the Certificate.

1.3.5 CERTIFICATE MANAGERS

As part of this CP/CPS, a Certificate Manager is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant and is responsible for the use of the certificate (and associated private key).

Certificate Managers must meet the conditions and obligations that are set in this CP/CPS and in the Subscriber Agreement. The Certificate is attached to the Subscriber and not to the Certificate Manager. In case of change of Certificate Manager, the Subscriber shall report it to NOSICA SSL and appoint a successor.

1.3.6 OTHER PARTICIPANTS

In the addition to the PKI participants described in Sections 1.3.2, 1.3.3 and 1.3.4, NOSICA SSL will involve other parties as needed. NOSICA SSL will contractually obligate each party to comply with all applicable requirements in this CP/CPS and monitor its compliance.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

SSL Certificates are used to secure online communication and transactions where the risks of data compromise and fraud exist. The SSL Certificate allows the end entity to prove its identity to other participants and maintaining the integrity of the transaction. At all times, Subscribers are required to use Certificates in accordance with this CP/CPS and all applicable laws and regulations.

1.4.2 PROHIBITED CERTIFICATE USES

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorized.

Certificates issued under this CP/CPS may not be used (i) for any application requiring fail safe performance such as (a) air traffic control systems, (b) aircraft navigation systems, (c) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

SSL Certificates issued under this CP/CPS do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment on which the Certificate has been installed is not free from defect, malware or virus.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The organization administering the CP/CPS is NOSICA SSL. Its Management Committee acts as the Certificate Policy Authority. The Management Committee is composed of the senior management of NOSICA SSL. The NOSICA SSL Management Committee is the highest-level management body with final authority and responsibility for:

- Specifying and approving the NOSICA SSL infrastructure and practices;
- Approving the NOSICA SSL CP/CPS;
- Defining the review process for practices and policies including responsibilities for maintaining the CP/CPS;
- Defining the review process that ensures that NOSICA SSL CAs properly implement the above practices;
- Publication to the Subscribers and Relying Parties of the CP/CPS and its revisions.

1.5.2 CONTACT PERSON

NOSICA SSL Certificate Policy Authority may be contacted at the following address:

NOSI – Edifício Business Center, Parque Tecnológico, C.P. 620, Achada Grande Frente, Praia, Cabo Verde
Tel.: +238 333 62 22/ 62 73
Mail: nosicert@nosi.cv
Web: <https://pki.nosi.cv/>

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can submit Certificate Problem reports of suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates via email to nosicert@nosi.cv. Further details are available in <https://pki.nosi.cv/web/guest/revoga%C3%A7%C3%A3o>.

1.5.3 PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY

The Management Committee is responsible for determining the suitability and applicability of this CP/CPS based on the results and recommendations received from a Qualified Auditor as specified in Section 8.

1.5.4 CP/CPS APPROVAL PROCEDURE

NOSICA SSL Management Committee will approve the CP/CPS, along with any amendments. Any amendments made to the CP/CPS will be reviewed by the Security Administration for consistency with the practices that are implemented prior to its approval. Changes made will be tracked within the revision table. Refer to Section 9.12 below for CP/CPS amendment procedure.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 DEFINITIONS

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, 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: 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 the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Report: 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 CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates.

Authorization Domain Name: The FQDN used to obtain authorization for Certificate issuance for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*" from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry controlled or public suffix plus the registry-controlled or public suffix

(e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates as published by the CA/Browser Forum and any amendments to such document.

CAA: From RFC 8659 (<http://tools.ietf.org/html/rfc8659>): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue Certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended Certificate mis-issue."

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Management System: A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Systems: The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross -Certified Subordinate CA Certificate: A Certificate that is used to establish a trust relationship between two CAs.

CSPRNG: A random number generator intended for use in a cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Delegated Third Party System: Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.

DNS CAA Email Contact: The email address defined in section A.1.1 of the Baseline Requirements.

DNS CAA Phone Contact: The phone number defined in Section A.1.2 of the Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Section A.2.1 of the Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Section A.2.2 of the Baseline Requirements.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499 (<https://tools.ietf.org/html/rfc8499>): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names those are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar

as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.

Domain Name Register: A person or entity that registers Domain Names under the auspices of or by agreement with:

- (i) the Internet Corporation for Assigned Names and Numbers (ICANN),
- (ii) a national Domain Name authority/registry, or
- (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date: The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.

Fully-Qualified Domain Name: A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, country, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected Certificate requests or revoked Certificates, names listed on the Miller

Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Individual: A natural person.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of Certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

LDH Label: From RFC 5890 (<https://tools.ietf.org/html/rfc5890>): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Linting: A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a `tbsCertificate` (as described in [RFC 5280, Section 4.1.1.1](#)) is checked for conformance with the profiles and requirements defined in the Baseline Requirements.

Multi-Factor Authentication: An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent. Certificate based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.

Multi-Perspective Issuance Corroboration: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

Network Perspective: Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

Non-Reserved LDH Label: From RFC 5890 (<https://tools.ietf.org/html/rfc5890>): "The set of valid LDH labels that do not have ' `--` ' in the third and fourth positions."

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Onion Domain Name: A Fully Qualified Domain Name ending with the RFC 7686 “.onion” Special-Use Domain Name. For example,
2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

Pending Prohibition: The use of a behavior described with this label is highly discouraged, as it is planned to be deprecated and will likely be designated as MUST NOT in the future.

Primary Network Perspective: The Network Perspective used by the CA to make the determination of 1) the CA’s authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant’s authority and/or domain authorization or control of the requested domain(s) or IP address(es).

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

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

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 of the CA/B Forum Baseline Requirements.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: 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: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate. Relying Parties must read and agree to NOSICA SSL's relying party agreement available at <https://pki.nosi.cv/repositorio>.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Note: Examples of Request Tokens include, but are not limited to:

- (i) a hash of the public key; or
- (ii) a hash of the Subject Public Key Info [X.509]; or
- (iii) a hash of a PKCS#10 CSR.

A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.

Note: This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. `echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr` \| sed "s/[-]/g".`

The script outputs:

201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Baseline Requirements of the CA/B Forum.

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:

<https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml>.

<https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml>.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures to be performed for the generation of the Root CA Key Pair.

Short-lived Subscriber Certificate: For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties available at <https://pki.nosi.cv/repositorio>.

Subsidiary Company: A company that is controlled by a Parent Company.

Technically Constrained Subordinate CA Certificate: A Subordinate CA Certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles of the Baseline Requirements to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Test Certificate: This is no longer used in the Baseline Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified by these Requirements.

Validity Period: From [RFC 5280](#): “The period of time from notBefore through notAfter, inclusive”.

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names contained in the Certificate.

Wildcard Domain Name: A string starting with “*.” (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

XN-Label: From RFC 5890 (<http://tools.ietf.org/html/rfc5890>): “The class of labels that begin with the prefix “xn--” (case independent), but otherwise conform to the rules for LDH labels.”

1.6.2 ACRONYMS

AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement

CV	Cabo Verde
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TSP	Trust Service Provider
VOIP	Voice Over Internet Protocol

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

NOSICA SSL makes the following available on its public repository at <https://pki.nosi.cv/repositorio>:

- NOSICA SSL CP/CPS;
- Subscriber contractual agreements (e.g: Subscriber Agreement, Application Forms, etc.);
- Audit Reports by Qualified Auditors;
- Certification Authority Certificates and related Authority Revocation Lists (ARLs);
- Certificate Revocation Lists (CRLs).

For further details regarding the publication of information refer to section 2.2.

NOSICA SSL ensures that revocation data for issued Certificates and its Root Certificates are available in accordance with the CP/CPS.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

NOSICA SSL conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at <http://www.cabforum.org>. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

NOSICA SSL publishes information mentioned in section 2.1 on its publicly accessible website <https://pki.nosi.cv/repositorio> that is available on a 24x7 basis.

In addition, NOSICA SSL publishes test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. These test Web pages are accessible at the following URLs:

- Valid Certificate: <https://validovssl.NOSICASSL.cv/>
- Revoked Certificate: <https://revokedovssl.NOSICASSL.cv/>
- Expired Certificate: <https://expiredovssl.NOSICASSL.cv/>

Prior to issuing SSL Certificates, NOSICA SSL checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued as specified in RFC 8659 as per Section 4.2.4. NOSICA SSL's CAA issuer domain is nosi.cv.

2.3 TIME OR FREQUENCY OF PUBLICATION

NOSICA SSL reviews its CP/CPS at least annually and makes appropriate changes so that NOSICA SSL CA operation remains accurate, transparent and complies with requirements listed in Section 8 of this document. NOSICA SSL CA closely monitors CA/Browser Forum ballots and updates to the Baseline Requirements and implements updates to NOSICA SSL operations in a timely manner.

Revision Table in Section 1.2 indicates reviews and updates made to this CP/CPS by adding a dated changelog entry and incrementing the CP/CPS version number, even if no other changes are made to the document.

New or modified versions of this CP/CPS, Subscriber Agreements, or Relying Party agreements are published within seven days after approval.

Publication frequency of CRLs and frequency of updating OCSP records are specified in Sections 4.9.7 and 4.9.9.

2.4 ACCESS CONTROLS ON REPOSITORIES

Read only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1. TYPES OF NAMES

The Subscriber is described in the Certificate by a Distinguished Name pursuant to the X.501 standard.

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

Any Fully-Qualified Domain Name (FQDN) which is embedded into a Certificate either as a DN component, or as a `dnsName` `subjectAltName` must conform to the standard semantics for DNS names described in RFC 1034. All DNS names embedded into an OV SSL Certificate issued by NOSICA SSL is restricted by the “.cv” top-level domain for Cabo Verde and owned by entities operating under the Capeverdean Jurisdiction.

Organizational names must be validated to be syntactically identical to an entry in the General Directorate of Registry, Notary and Identification as was used to validate the certificate request.

If the combination of names or the organization name by itself exceeds 64 characters, NOSICA SSL abbreviates parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that NOSICA SSL checks this field in accordance with section 3.2.2.10 and a Relying Party will not be misled into thinking that they are dealing with a different organization.

3.1.3. ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

NOSICA SSL does not issue anonymous or pseudonymous Certificates.

3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

Fields contained in SSL Certificates are in compliance with this CP/CPS. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs.

3.1.5. UNIQUENESS OF NAMES

The full combination of the Subject Attributes (DN) is unique within the boundaries defined by this CP/CPS and conforms to all applicable X.500 standards for the uniqueness of names. The `SerialNumber` attribute guarantees the uniqueness of the DN in the Certificate.

3.1.6. RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

NOSICA SSL will only issue certificates that include trademarks if the trademark is registered with the National Trademark Office. NOSICA SSL will not issue certificates with trademarks that are not documented at the National Entity responsible for the Registration of Trademarks.

3.2 INITIAL IDENTITY VALIDATION

NOSICA SSL performs identification of the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity and individual.

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The Applicant provides a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in an SSL Certificate. NOSICA SSL parses the PKCS#10 CSR submitted by the Applicant and verifies that the Applicant's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR.

3.2.2. AUTHENTICATION OF ORGANIZATION AND DOMAIN IDENTITY

NOSICA SSL issues SSL Certificates for public and private organizations and verify the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3.

NOSICA SSL verifies the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of Section 3.2.2.1. NOSICA SSL inspects any document relied upon for alteration or falsification.

3.2.2.1 IDENTITY

NOSICA SSL verifies the existence and identity of the organization using the following methods:

- For Ministries and administrative public enterprises: NOSICA SSL will obtain an excerpt from Official Gazette of the Republic of Cape Verde that proves the legal existence of the entity. Other information such as the address of the entity and the

identity of the assigned responsible of the entity are verified based on other legal documents and official correspondences with the requesting agency or a superior government entity.

- For non-administrative public enterprises and private entities: NOSICA SSL will obtain the information from the General Directorate of Registry, Notary and Identification. The information extracted from the General Directorate of Registry, Notary and Identification includes at a minimum the legal name, legal address, tax identification number, first name and last name of the legal representative.

Alternatively, NOSICA SSL may verify the address, the phone number or email address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, Cabo Verde Yellow Pages or other form of identification that the CA determines to be reliable.

In order to validate the relationship of a physical person requesting an SSL certificate with the organization, the following information is required:

- The information in the National Identity Card (for Capeverdeans), obtained through a verification tool based on webservices of governmental entities put at the disposal of the RA operator, or a copy of the passport or Cabo Verde residency card (for foreigners) of one of the physical persons who is a legal representative of the organization.
- The information in the National Identity Card (for Capeverdeans), obtained through a verification tool based on webservices of governmental entities put at the disposal of the RA operator, or a copy of the passport or Cabo Verde residency card (for foreigners) of the Certificate Manager.

3.2.2.2 DBA/TRADENAME

If the Subject Identity Information is to include a DBA or tradename, NOSICA SSL verifies the Applicant's right to use the DBA/tradename using at least one of the following:

- A recent extract from the Capeverdean National Register of Enterprises not older than 3 months;

- Communication with a government entity responsible for the management of such DBAs or trade names.

The registered DBA/tradename in official document must match the claimed DBA/tradename exactly.

3.2.2.3 VERIFICATION OF COUNTRY

If the subject: countryName field is present, then the NOSICA SSL verify the country associated with the Subject using one of the following:

- a. the IP Address range assignment by country for either
 - i. the web site's IP address, as indicated by the DNS record for the web site
or
 - ii. the Applicant's IP address;
- b. the ccTLD of the requested Domain Name;
- c. information provided by the Domain Name Registrar; or
- d. a method identified in Section 3.2.2.1.

3.2.2.4 VALIDATION OF DOMAIN AUTHORIZATION OR CONTROL

NOSICA SSL confirms that prior to issuance, NOSICA SSL has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below. NOSICA SSL does not issue certificates with a FQDN that contain "onion" as the rightmost Domain Label.

NOSICA SSL maintains a record of which domain validation method, including relevant Baseline Requirements version number that was used to validate every domain.

3.2.2.4.1 VALIDATING THE APPLICANT AS A DOMAIN CONTACT

NOSICA SSL does not use this method.

3.2.2.4.2 EMAIL, FAX, SMS, OR POSTAL MAIL TO DOMAIN CONTACT

NOSICA SSL does not use this method.

3.2.2.4.3 PHONE CONTACT WITH DOMAIN CONTACT

NOSICA SSL does not use this method.

3.2.2.4.4 CONSTRUCTED EMAIL TO DOMAIN CONTACT

NOSICA SSL confirms the Applicant's control over the FQDN or Wildcard Domain names by:

- a) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,
- b) including a Random Value in the email, and
- c) receiving a confirming response utilizing the Random Value.

This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the domain name.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The email with no content and no recipient modification may be re-sent in its entirety, including the re-use of the Random Value. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, NOSICA SSL may also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 DOMAIN AUTHORIZATION DOCUMENT

NOSICA SSL does not use this method.

3.2.2.4.6 AGREED-UPON CHANGE TO WEBSITE

NOSICA SSL does not use this method.

3.2.2.4.7 DNS CHANGE

NOSICA SSL confirms the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either

- a) an Authorization Domain Name; or
- b) an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character.

If a Random Value is used, NOSICA SSL provides a Random Value unique to the Certificate request and does not use the Random Value after:

- i. 30 days or
- ii. if the Applicant submitted the Certificate request, the time frame permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of the Baseline Requirements).

NOSICA SSL implement Multi-Perspective Issuance Corroboration as specified in [Section 3.2.2.9](#) of the Baseline Requirements to count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, NOSICA SSL may also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP ADDRESS

NOSICA SSL does not use this method.

3.2.2.4.9 TEST CERTIFICATE

NOSICA SSL does not use this method.

3.2.2.4.10 TLS USING A RANDOM VALUE

NOSICA SSL does not use this method.

3.2.2.4.11 ANY OTHER METHOD

NOSICA SSL does not use any other method.

3.2.2.4.12 VALIDATING APPLICANT AS A DOMAIN CONTACT

NOSICA SSL does not use this method.

3.2.2.4.13 EMAIL TO DNS CAA CONTACT

NOSICA SSL may confirm the Applicant's control over the FQDN by sending a Random Value via email to a DNS CAA Email Contact. This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the Domain Name.

In this case, the relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 Section 3.

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value is unique in each email. NOSICA SSL may re-send the email in its entirety, including the reuse of the Random Value, provided that its entire contents and recipient(s) remain unchanged. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

NOSICA SSL implement Multi-Perspective Issuance Corroboration as specified in [Section 3.2.2.9](#) of the Baseline Requirements. To count as corroborating, a Network Perspective observes the selected contact address used for domain validation observed by the Primary Network Perspective.

Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.14 EMAIL TO DNS TXT CONTACT

NOSICA SSL may confirm the Applicant's control over the FQDN by sending a Random Value via email. This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the domain name.

In this case, the Random Value is sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email may confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value is unique in each email. NOSICA SSL may re-send the email in its entirety, including the reuse of the Random Value, provided that its entire contents and recipient(s) remain unchanged. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

NOSICA SSL implement Multi-Perspective Issuance Corroboration as specified in [Section 3.2.2.9](#) of the Baseline Requirements. To count as corroborating, a Network Perspective observes the selected contact address used for domain validation observed by the Primary Network Perspective.

Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.15 PHONE CONTACT WITH DOMAIN CONTACT

NOSICA SSL does not use this method.

3.2.2.4.16 PHONE CONTACT WITH DNS TXT RECORD PHONE CONTACT

NOSICA SSL does not use this method.

3.2.2.4.17 PHONE CONTACT WITH DNS CAA PHONE CONTACT

NOSICA SSL does not use this method.

3.2.2.4.18 AGREED-UPON CHANGE TO WEBSITE V2

NOSICA SSL does not use this method.

3.2.2.4.19 AGREED-UPON CHANGE TO WEBSITE – ACME

NOSICA SSL does not use this method.

3.2.2.4.20 TLS USING ALPN

NOSICA SSL does not use this method.

3.2.2.5 AUTHENTICATION FOR AN IP ADDRESS

NOSICA SSL does not issue certificates with IP addresses.

3.2.2.6 WILDCARD DOMAIN VALIDATION

If a Wildcard Domain Name is to be included in a Certificate, then NOSICA SSL issuing CAs remove "*" from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. NOSICA SSL issuing CAs may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Before issuing a Wildcard Certificate, NOSICA SSL follow an internal documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is "registry-controlled".

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", the NOSICA SSL issuing CAs refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7 DATA SOURCE ACCURACY

NOSICA SSL prior to using any data source as a Reliable Data Source, evaluate the source for its accuracy and resistance to alteration or falsification.

Before relying on any data provided, NOSICA SSL will verify the following attributes:

- The age of the information provided,
- The frequency of updates to the information source,

- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA RECORDS

As part of the Certificate issuance process, NOSICA SSL retrieves and processes CAA records in accordance with RFC 8659 for each `dNSName` in the `subjectAltName` extension that does not contain an Onion Domain Name. If NOSICA SSL issues a Certificate after processing a CAA record, it does so within the TTL of the CAA record, or 8 hours, whichever is greater.

Some of the methods used to validate the Applicant's ownership or control of the subject domain(s) used by NOSICA SSL require that CAA records be retrieved and processed from additional remote Network Perspectives prior to issuance of the Certificate, in order to corroborate the Primary Network Perspective.

NOSICA SSL takes the CAA verification response from a remote Network Perspective and interprets it as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. In addition, NOSICA SSL considers the response from a remote Network Perspective to be corroborative if one or both Perspectives have an acceptable CAA record lookup failure, as defined in this section.

NOSICA SSL MAY check CAA records at any other time.

When processing CAA records, NOSICA SSL processes the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. NOSICA SSL respects the critical flag and not issue a certificate if it encounters an unrecognized property tag with this flag set.

If the CA issues a certificate after processing a CAA record, it MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

RFC 8659 requires that CAs "MUST NOT issue a certificate unless the CA determines that either (1) the certificate request is consistent with the applicable CAA RRset or (2) an exception specified in the relevant CP or CPS applies." For issuances conforming to the Baseline Requirements, NOSICA SSL does not rely on any exceptions specified in this CP or CPS unless they are one of the following:

- CAA checking is optional for certificates for which a Certificate Transparency Precertificate (see Section 7.1.2.9) was created and logged in at least two public logs, and for which CAA was checked at time of Precertificate issuance.
- CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Section 7.1.2.3 or Section 7.1.2.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

NOSICA SSL is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside NOSICA SSL's infrastructure; and
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

NOSICA SSL documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances, and endeavors to dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. NOSICA SSL is not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.2.9 MULTI-PERSPECTIVE ISSUANCE CORROBORATION

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

NOSICA SSL use either the same set, or different sets of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required 1) Domain Authorization or Control and 2) CAA Record checks.

The set of responses from the relied upon Network Perspectives **MUST** provide NOSICA SSL with the necessary information to allow it to affirmatively assess: - a. the presence of the expected 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the relied upon validation method specified in Sections 3.2.2.4 and 3.2.2.5; and - b. the NOSICA SSL's authority to issue to the requested domain(s), as specified in Section 3.2.2.8.

Section 3.2.2.4 and Section 3.2.2.5 describe the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a Network Perspective can corroborate the outcomes determined by the Primary Network Perspective.

Results or information obtained from one Network Perspective are not reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). The network infrastructure providing Internet connectivity to a Network Perspective **MAY** be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and NOSICA SSL take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective **MAY** use a recursive DNS resolver that is **NOT** co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective **MUST** fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two States, Provinces, or Countries the DNS resolvers reside in **MUST** be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

NOSICA SSL immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method. When retrying Multi-Perspective Issuance Corroboration, NOSICA SSL DO NOT rely on corroborations from previous attempts.

The “Quorum Requirements” Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If NOSICA SSL does NOT rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements MUST be met for both sets of Network Perspectives (i.e., the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between the two States, Provinces or Countries they reside in is at least 500 km. Network Perspectives are considered “remote” when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

NOSICA SSL MAY reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives MAY omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

NOSICA SSL uses Remote Network Perspectives performing Multi-Perspective Issuance Corroboration as set out in section 3.2.2.9 of the Baseline Requirements document.

3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY

NOSICA SSL does not issue SSL certificates to natural person. However, as part of the certificate application process, NOSICA SSL will verify the identity of the Certificate Manager and the legal representative of the organization as detailed in Section 3.2.2.1.

The Certificate Manager is either the Legal Representative of the entity or a natural person formally designated by the Legal Representative. The designation of a Certificate Manager is performed simultaneously with the submission of the SSL Certificate Application Form.

As mentioned in Section 4.1.2, the Certificate Application Form is signed by : (i) the Legal Representative to mandate the future Certificate Manager and (ii) the future Certificate Manager to accept this role and the Subscriber Agreement.

NOSICA SSL 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). NOSICA SSL inspect the copy for any indication of alteration or falsification.

NOSICA SSL verify the Applicant's address using a government ID, utility bill, or bank or credit card statement. NOSICA SSL rely on the same government-issued ID that was used to verify the Applicant's name.

NOSICA SSL verify the certificate request with the Applicant using a Reliable Method of Communication.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Unverified information is never included in NOSICA SSL end entities Certificates. All Subscriber information included in Certificates are duly verified.

3.2.5. VALIDATION OF AUTHORITY

This step is performed simultaneously with the validation of the identity of the Legal Representative and of the Certificate Manager. As mentioned in Section 3.2.3, the certificate application form is signed by the legal representative of the entity and the certificate manager and each of them must provide a copy of his or her ID. Signatures of the Legal Representative and Certificate Manager must be a legally valid and contain an enforceable seal or handwritten signature or be a legally valid and enforceable electronic signature.

In addition, NOSICA SSL uses a Reliable Method of Communication derived from the verification process described in section 3.2.2.1 to establish the authenticity of the certificate request directly with the Applicant Legal Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices,

corporate offices, human resource offices, information technology offices, or other department that NOSICA SSL deems appropriate.

3.2.6 CRITERIA FOR INTEROPERATION

NOSICA SSL does not have any Cross-Certified Subordinate CA Certificates with other CAs.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Not Applicable. NOSICA SSL does not support re-key.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Not Applicable. NOSICA SSL does not support re-key.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests are authenticated to ensure they emanate from authorized people. The process how the revocation request can be submitted is described in Section 4.9.3.

NOSICA SSL may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non-payment of applicable fees.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Applicants must comply with provisions set within the registration forms and processes, this CP/CPS and the Subscriber Agreement.

NOSICA SSL maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. NOSICA SSL uses this information to identify individuals from whom and entities from which it will not accept Certificate applications.

In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which NOSICA SSL operates are used to screen out unwanted Applicants.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

NOSICA SSL makes available to Applicants all required Application forms as well as all applicable Subscriber Agreements: (i) on its public repository at <https://pki.nosi.cv/repositorio>, (ii) by email to nosicert@nosi.cv, (iii) and within its headquarters (see Section 1.5.2).

Prior to the issuance of a Certificate, NOSICA SSL obtains a dully filled and signed Application Form that falls into five parts as described hereafter:

- Part 1 : Applicant details including legal name, tax identification number, a telephone number, email address, and postal delivery address;
- Part 2 : Legal Representative details including full name, ID Number, telephone number and email address;
- Part 3 : Certificate Manager details including full name, ID Number, telephone number and email address;
- Part 4 : Certificate type; Certificate Validity, FQDN Names to embed into the SSL Certificate;

- Part 5 : Signature of the Legal Representative and the Certificate Manager by which they confirm their acceptance and compliance with the Subscriber Agreement.

The Applicant commits to providing a current, genuine and complete certificate request and all evidence requested by NOSICA SSL. The paper Application, with the Applicant wet seal and handwritten signatures of the Applicant's legal representative and the Certificate Manager, must be physically submitted to a NOSICA SSL RA.

Applicant may submit electronic Application Form with the digital signature of the Applicant Legal Representative and the Certificate Manager. The digital signatures of Legal Representative and Certificate Manager must be compliant to the Capeverdean Law related to digital signature.

The certificate request **MUST** contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

The Applicant generates the key pair by itself and creates a Certificate Signing Request (CSR) as to prove that the private key belongs to itself and sends this to NOSICA SSL RA from email address used to verify domain control or provides it to NOSICA SSL RA operator on a hardware device (CD, USB Token). The Applicant is responsible for taking all required measures for protecting confidentiality and integrity of its private key.

NOSICA SSL's responsibility is to verify and to validate the information supplied. This will be done in compliance with the practices stated in this CP/CPS and by strictly following the NOSICA SSL registration procedures and the applicable national laws.

NOSICA SSL guarantees that all required verifications have been performed prior to successful registration leading to Certificate issuance and that all certificate requests submitted to the Issuing CAs are complete, accurate, valid and duly authorized. It also guarantees the accuracy of all information contained in the Certificate.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Applications for OV SSL Certificates shall be submitted by the legal representative of the organization who owns the Domain Name.

OV SSL Certificate application includes the following:

- Order Form including the Subscriber Agreement as described in Section 4.1.
- Documents proving the legal existence of the Applicant if the Organization does not have a Capeverdean National Register of Enterprises (Section 3.2.2),
- Copy of the ID of the legal representative if he/she does not have the Capeverdean nationality (passport or Cabo Verde residency card),
- Copy of the ID of the Certificate Manager if he/she does not have the Capeverdean nationality (passport or Cabo Verde residency card),
- The Certificate Signing Request (CSR) that includes at least one Fully-Qualified Domain Name to be included in the Certificate's subjectAltName extension.

For DV SSL Certificates applications, NOSICA SSL performs all identification and authentication functions in accordance with this CP/CPS. This includes validation per Section 3.2.2.

Certificate information is verified using data and documents obtained no more than 90 days prior to issuance of the Certificate.

As part of the validation process, NOSICA SSL checks for CAA records for each requested DNS name and follows the processing instructions found as specified in RFC 8659 and Section 3.2.2.8 of the Baseline Requirements. The CA acts in accordance with CAA records if present. If the CA issues, it does so within the TTL of the CAA record, or 8 hours, whichever is greater. The CA's CAA identifying domain is pki.nosi.cv.

NOSICA SSL maintains a list of high-risk domains and blocks issuance of certificates for those domains. Requests for removal from the high-risk domains list are considered, but

generally require further documentation confirming control of the domain from the Applicant, or other proof as NOSICA SSL deems necessary.

The following verification tasks are performed by NOSICA SSL's RA:

- Validation of the identity and the legal existence of the Applicant (Section 3.2.2):
The Applicant must be a legal entity;
- Validation of the identity of the legal representative and the Certificate Manager (section 3.2.2);
- Validation of domain control (section 3.2.2.4);
- Assurance that the certificate request does not fall into high risk or blacklisted certificate requests;
- Verification of CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued (Section 3.2.2.8).

NOSICA SSL does not re-use previous validation information. Each certificate application must go through all validation functions described in section 3.2. End-user Certificate validity is specified in Section 6.3.2.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

NOSICA SSL will approve or reject an Applicant's Certificate request based upon the Applicant meeting the requirements of this CP/CPS and all applicable laws and regulations.

NOSICA SSL rejects any certificate application that NOSICA SSL cannot verify. NOSICA SSL does not issue certificates containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.2.4 or Section 3.2.2.5.

NOSICA SSL, in its sole discretion, may reject a Certificate Application, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. NOSICA SSL reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

NOSICA SSL, at its sole discretion not to be unreasonably withheld, may override any decision to Approve Applicant's Certificate request.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Under normal circumstances, NOSICA SSL confirms Certificate application information and issues a Certificate within seven working days as established by Capeverdean national law.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

4.3.1.1 MANUAL AUTHORIZATION OF CERTIFICATE ISSUANCE FOR ROOT CAS

Not Applicable.

4.3.1.2 LINTING OF TO-BE-SIGNED CERTIFICATE CONTENT

Upon receipt of an approved Certificate signing request, NOSICA SSL proceeds to the Certificate issuance process.

Certificate issuance by NOSICA SSL requires a NOSICA SSL RA operator in a Trusted Role authorized by NOSICA SSL to deliberately issue a direct command in order for NOSICA SSL to perform a certificate signing operation. The RA operators accounts capable of causing certificate issuance or performing Registration Authority functions are enforced with multi-factor authentication (certificate in cryptographic token + PIN code). Technical controls are operated by NOSICA SSL in order to restrict certificate issuance through accounts to a limited set of pre-approved email addresses. Each issuance is logged with the identity of the NOSICA SSL RA operator issuing the certificate and the action is logged in the CA audit log.

Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

Due to the complexity involved in implementing Certificate Profiles that conform to the Baseline Requirements, NOSICA SSL implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that the CA has a technical control to verify that the to-be-

signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962, Section 3.2.

NOSICA SSL uses an automated issuance process that integrates pre-issuance linting tools, kept up-to-date, which can check a tbsCertificate (To Be Signed Certificate - the certificate complete except for the signature) for a large number of standards violations (Baseline Requirements, RFCs, etc.). Certificate issuance is held up for manual review if a linting error or warning is found. The linting error is flagged and brought to the attention of management to complete further internal verification and final decision on the certificate issuance.

NOSICA SSL uses the Linting tools that have been widely adopted by the industry (see <https://cabforum.org/resources/tools/>).

NOSICA SSL will contribute, when possible, to open-source Linting projects, such as by:

- creating new or improving existing lints,
- reporting potentially inaccurate linting results as bugs,
- notifying maintainers of Linting software of checks that are not covered by existing lints, - updating documentation of existing lints, and
- generating test certificates for positive/negative tests of specific lints.

4.3.1.3 LINTING OF ISSUED CERTIFICATES

NOSICA SSL may use a Linting process to test each issued Certificate.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The Applicant will be notified that the Certificate is issued via the Certificate Manager email address that was supplied by the Subscriber during the enrollment process and will be provided with appropriate instructions on how to obtain the Certificate. If the Certificate is presented to the Subscriber immediately, special notification may not be necessary.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

A Subscriber that accepts a Certificate warrants to NOSICA SSL, that all information supplied in connection with the application process and all information included in the Certificate issued to them is true, complete, and not misleading.

Without limitation to the generality of the foregoing, the use of a Certificate signifies acceptance by that Subscriber of this CP/CPS and Subscriber Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

If the subscriber is not satisfied with the details contained within the certificate, he or she must email pki@nosi.cv explaining why the certificate is not being accepted. This communication must take place within 30 days of issuance.

Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Refer to Section 2.1.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Other than Certificate Transparency publication, NOSICA SSL does not notify other entities of certificate issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers have to protect their Private Key to avoid disclosure to third parties. NOSICA SSL provides a Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection.

Subscribers are bound to use the Certificate for its lawful and intended purposes only.

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

Within this CP/CPS, NOSICA SSL provides the conditions under which Certificates may be relied upon by Relying Parties including the appropriate Certificate services available to verify Certificate validity such as CRL and/or OCSP.

In order to be a Relying Party, a Party seeking to rely on a Certificate issued by NOSICA SSL CA agrees to and accepts the Relying Party Agreement available at <https://pki.nosi.cv/repositorio> by querying the existence or validity of; or by seeking to place or by placing reliance upon a Certificate.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS,
- That the Certificate is being used in accordance with its Key-Usage field extensions,
- That the Certificate is valid at the time of reliance by reference to OCSP or CRL Checks.

4.6 CERTIFICATE RENEWAL

Certificate renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate. Certificate renewal is not supported by NOSICA SSL.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Not Applicable. Certificate renewal is not supported by NOSICA SSL.

4.6.2 WHO MAY REQUEST RENEWAL

Not Applicable. Certificate renewal is not supported by NOSICA SSL.



4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Not Applicable. Certificate renewal is not supported by NOSICA SSL.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. Certificate renewal is not supported by NOSICA SSL.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Not Applicable. Certificate renewal is not supported by NOSICA SSL.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Not Applicable. Certificate renewal is not supported by NOSICA SSL.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. Certificate renewal is not supported by NOSICA SSL.

4.7 CERTIFICATE RE-KEY

Certificate re-key means the issuance of a new certificate with a new public key, but with the same subject identity information. NOSICA SSL does not support re-key.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Not Applicable. NOSICA SSL does not support re-key.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Not Applicable. NOSICA SSL does not support re-key.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Not Applicable. NOSICA SSL does not support re-key.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. NOSICA SSL does not support re-key.



4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Not Applicable. NOSICA SSL does not support re-key.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Not Applicable. NOSICA SSL does not support re-key.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. NOSICA SSL does not support re-key.

4.8 CERTIFICATE MODIFICATION

Certificate modification is the process through which a Subscriber requests a Certificate with modified subject information. NOSICA SSL considers such request as an initial registration request. The requester is therefore required to start a new Certificate request.

4.8.1 CIRCUMSTANCES FOR CERTIFICATE MODIFICATION

Not Applicable. NOSICA SSL does not support Certificate modification.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Not Applicable. NOSICA SSL does not support Certificate modification.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Not Applicable. NOSICA SSL does not support Certificate modification.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. NOSICA SSL does not support Certificate modification.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

Not Applicable. NOSICA SSL does not support Certificate modification.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

Not Applicable. NOSICA SSL does not support Certificate modification.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. NOSICA SSL does not support Certificate modification.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 CIRCUMSTANCES FOR REVOCATION

Certificate revocation is the process by which NOSICA SSL prematurely terminates the Validity of a Certificate. NOSICA SSL will make its certificate revocations public through the use of publicly issued CRLs and publicly available OCSP responder services.

4.9.1.1 REASONS FOR REVOKING A SUBSCRIBER CERTIFICATE

With the exception of Short-lived Subscriber Certificates, NOSICA SSL revokes a Certificate within 24 hours and uses the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLReason, that NOSICA SSL revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies NOSICA SSL that the original Certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. NOSICA SSL obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. NOSICA SSL is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in 6.1.1.3 (CRLReason #1, keyCompromise);
5. NOSICA SSL obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

With the exception of Short-lived Subscriber Certificates, NOSICA SSL revokes a Certificate within 5 days and uses the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 (CRLReason #4, superseded);
2. NOSICA SSL obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
3. NOSICA SSL is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement (CRLReason #9, privilegeWithdrawn);
4. NOSICA SSL is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
5. NOSICA SSL is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
6. NOSICA SSL is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
7. NOSICA SSL is made aware that the Certificate was not issued in accordance with the Baseline Requirements or the present CP/CPS (CRLReason #4, superseded);
8. NOSICA SSL determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
9. NOSICA SSL's right to issue Certificates under these Requirements expires or is revoked or terminated, unless NOSICA SSL has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

10. Revocation is required by this CP/CPS for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
11. NOSICA SSL is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 REASONS FOR REVOKING A SUBORDINATE CA CERTIFICATE

NOSICA SSL does not have any third party Subordinate CAs. The only CAs that NOSICA SSL operates are the ones listed in section 1.3.1.

4.9.2 WHO CAN REQUEST REVOCATION

NOSICA SSL accepts authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or its appropriately authorized Certificate Manager.

Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify NOSICA SSL of a suspected reasonable cause to revoke the Certificate. Problem Reports shall be submitted to the Contact Person specified in Section 1.5.2. NOSICA SSL may also at its own discretion revoke Certificates.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

A revocation request should be promptly and directly communicated to NOSICA SSL. A revocation request may be submitted using one of the following methods:

- Using NOSICA SSL revocation online service available at <https://pki.nosi.cv/web/guest/revogação>. In this case, the Subscriber is required to provide:
 - o The FQDN listed in the certificate that needs to be revoked, and
 - o An email address to confirm the Subscriber's control over the listed FQDN, as per section 3.2.2.4.2 and section 3.2.2.4.4 of the present CP/CPS. A

revocation challenge will be sent to this email and the Subscriber needs to provide it for the certificate revocation to be processed.

- Physical presence before a NOSICA SSL RA operator: Either the Certificate Manager or the Legal Representative of the Subscriber must be physically present at the headquarters (Section 1.5.2) of NOSICA SSL and request the revocation of a Certificate in writing after providing a valid ID.

For Certificate Problem Report submitted by third parties to the Contact Person specified in Section 1.5.2, NOSICA SSL personnel begins investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:

- The nature of the alleged problem,
- The evidence provided in support of the request,
- The urgency of the request,
- The number of reports received about a particular certificate or website,
- The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered),
- and Capeverdean National Legislation.

4.9.4 REVOCATION REQUEST GRACE PERIOD

No grace period is permitted once a revocation request has been verified. NOSICA SSL will revoke Certificates according to sections 4.9.1.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

Within 24 hours after receiving a Certificate Problem Report, NOSICA SSL will investigate the facts and circumstances related to the Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, NOSICA SSL will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which NOSICA SSL will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation does not exceed the time frame set forth in Section 4.9.1.1.

The date selected by NOSICA SSL consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
5. Relevant legislation.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Relying parties must validate every Certificate against the most updated CRL as minimum. Alternatively, relying parties may check Certificate status using OCSP.

4.9.7 CRL ISSUANCE FREQUENCY

CRLs are available via a publicly-accessible HTTP URL (i.e., "published") as stated in Appendix B.

Within twenty-four (24) hours of issuing its first Certificate, NOSICA SSL generates and publishes a full and complete CRL.

NOSICA SSL issuing Subscriber Certificates:

- a) update and publish a new CRL at least every:
 - seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod (“AIA OCSP pointer”); or
 - four (4) days in all other cases;
- b) update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

4.9.8 MAXIMUM LATENCY FOR CRLS

The CRLs of NOSICA SSL are issued according to section 4.9.7 and published in a timely manner. The revocation becomes effective immediately upon its publication.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

The validity interval of an OCSP response is the difference in time between the `thisUpdate` and `nextUpdate` field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

A certificate serial is "assigned" if:

- a Certificate or Precertificate with that serial number has been issued by the Issuing CA; or
- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with the Issuing CA.

A certificate serial is "unassigned" if it is not "assigned".

The following applies for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

The OCSP responder operated by NOSICA SSL supports the HTTP GET method as described in RFC 6960 and/or RFC 5019. NOSICA SSL process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954.

For the status of Subscriber Certificate or its corresponding Precertificate:

- an authoritative OCSP response is available (i.e. the responder DO NOT respond with the “unknown” status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.
- NOSICA SSL OCSP responses have a validity interval greater than or equal to eight hours;
- NOSICA SSL OCSP responses have a validity interval less than or equal to ten days;
- NOSICA SSL OCSP responses have validity intervals less than sixteen hours, therefore NOSICA SSL updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

The following applies for communicating the status of all Certificates for which an OCSP responder is willing or required to respond.

NOSICA SSL OCSP responses conform to RFC6960 and/or RFC5019. OCSP responses are signed by an OCSP Responder which complies with the OCSP Responder Certificate Profile in Section 7.1.2.8.

If the OCSP Responder receives a request for the status of a Certificate serial number that is "unassigned", then the responder does not respond with a "good" status.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

NOSICA SSL supports OCSP responses in addition to CRLs. Relying Parties must confirm revocation information otherwise all warranties become void.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

NOSICA SSL does not employ any method other than OCSP and CRL for advertising revocation status.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

Should a Private Key become compromised, the related Certificate shall immediately be revoked. Should the private CA key become compromised, all Certificates issued by that CA shall be revoked.

In order to demonstrate Key Compromise, Parties must submit Certificate problem reports to NOSICA SSL (refer to section 1.5.2) that include one of the following methods:

- Submission of a signed CSR signed by the compromised Private Key and verifiable by the Public Key,
- Providing the Private Key itself,
- Providing references to vulnerability and/or security incident sources from which the Key Compromise is verifiable.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

No suspension of Certificates is performed by NOSICA SSL.

4.9.14 WHO CAN REQUEST SUSPENSION

No suspension of Certificates is performed by NOSICA SSL.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No suspension of Certificates is performed by NOSICA SSL.

4.9.16 LIMITS ON SUSPENSION PERIOD

No suspension of Certificates is performed by NOSICA SSL.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

NOSICA SSL provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both in the Certificates. NOSICA SSL does not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.10.2 SERVICE AVAILABILITY

NOSICA SSL operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of five seconds or less under normal operating conditions.

NOSICA SSL maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by NOSICA SSL.

NOSICA SSL maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 OPTIONAL FEATURES

The OCSP Responder is available for all types of certificates issued by NOSICA SSL.

4.11 END OF SUBSCRIPTION

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire.

4.12 KEY ESCROW AND RECOVERY

The private keys for each CA Certificate were generated and are stored in Hardware Security Modules (HSM) and are backed up but not escrowed.

4.12.1. KEY ESCROW AND RECOVERY POLICY AND PRACTICES

NOSICA SSL CA key-recovery is based on HSM standard key-backup where the keys in the backup are protected with encryption mechanism. All HSM backups and administrator smartcards are stored in a safety vault. Only persons performing trusted roles have the access to the safety vault.

NOSICA SSL does not store copies of Subscriber private keys; Subscriber's key back-up, escrow and key recovery are not possible.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

NOSICA SSL does not provide session key encapsulation and recovery.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

NOSICA SSL develops, implements, and maintains a comprehensive information security policy designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to NOSICA SSL by law.

The Certificate Management Process includes:

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. Network security and firewall management, including port restrictions and IP address filtering;
4. User management, separate trusted-role assignments, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

NOSICA SSL performs an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that NOSICA SSL has in place to counter such threats.

Based on the Risk Assessment, NOSICA SSL develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan also takes into account then-available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1. PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

NOSICA SSL data center exhibits the following features:

1. Protected with physical barriers, including solid walls that extend from real floor to real ceiling to prevent unauthorized entry and environmental contamination to the

CAs certificate manufacturing facility. Not located in areas likely to exhibit hazard of environmental damage, chemical, biological or radiological pollution,

2. Physically separated areas for visitor reception, clearance and computer equipment hosting,
3. Capable of safely storing, separate to any computer equipment, fuel to power facilities in the event of loss of mains power.

5.1.2 PHYSICAL ACCESS

Entry to NOSICA SSL Data Center containing the CA certificate manufacturing facility is achieved only through a limited number of access points controlled by security personnel on duty full time (24 hours per day, 365 days per year), and Intruder detection systems.

All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

The secure parts of NOSICA SSL hosting facilities are protected using physical access controls with biometric scanners or card access systems making them accessible only to appropriately authorized individuals. CA operational facilities are physically locked and alarmed when unoccupied.

All personnel and visitors entering and leaving CA operational facilities are logged. Entry, exit, and activities within CA facilities are under constant video surveillance. Third party support services personnel are granted restricted access to secure CA operational facilities only when required and such access is authorized and accompanied. Access rights to CA facilities are regularly reviewed and updated.

5.1.3 POWER AND AIR CONDITIONING

NOSICA SSL operates within data centers that have primary and secondary power supplies to ensure continuous, uninterrupted access to electric power. Redundant backup power is provided by battery uninterruptible power supplies (UPS) and one generator.

NOSICA SSL data center is equipped with heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 WATER EXPOSURES

The data center is in an area with no risk of flooding. The NOSICA SSL certificate manufacturing facility has a sealed roof to prevent exposure to water. HVAC systems are installed to prevent moisture build-up. The data center has policies that prevent liquids (e.g. drinks) from entering cabinet areas.

5.1.5 FIRE PREVENTION AND PROTECTION

NOSICA SSL has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke.

Fire doors exist on security perimeters around CA operational facilities and are alarmed.

NOSICA SSL's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 MEDIA STORAGE

All media containing production software and data, audit, archive, or backup information are stored within NOSICA SSL facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage such as water, fire, and electromagnetic.

5.1.7 WASTE DISPOSAL

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance to the manufacturer s' guidance prior to disposal.

5.1.8 OFF-SITE BACKUP

NOSICA SSL maintains copies of CA private keys, archived audit logs, and other sensitive information at secured off-site locations. All copies of private keys are stored in a system or device validated as meeting FIPS 140 Level 3 to ensure that they are only accessible by trusted personnel.

5.2. PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

NOSICA SSL personnel in trusted roles include, but are not limited to, CA and system administration personnel and personnel involved with customer support and vetting. An additional role to NOSICA SSL is the Auditor role, performed by NOSICA SSL's internal auditors.

The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of NOSICA SSL. All personnel appointed to a trusted role had a background check prior to allowing such person to act in a trusted role. A list of personnel appointed to trusted roles is maintained and reviewed at least annually.

The following roles are deemed to be trusted roles:

Management Committee	It is responsible for appointing the members of the other groups and for making critical decisions for the CE. This
----------------------	---



	<p>group must be made up of a minimum of 3 (three) members who are appointed by the NOSI EPE board of directors.</p> <p>The responsibilities of this group are</p> <ul style="list-style-type: none">a) Review and approve the policies proposed by the Security Management working group;b) Appoint the members of the other working groups;c) Make the identification of all individuals belonging to the various working groups available in one or more places that are easily accessible to authorized individuals;d) Manage the Management Environment;e) Disseminate new policies to the other members of the Groups;f) Making critical decisions about the operation of the CE;g) Replacing a set of administrator cards. This operation only needs to be carried out if you want to increase or reduce the number of administrator cards;h) Replacing a set of operator cards. This operation is only necessary if you want to increase or reduce the number of operator cards or replace a damaged card;i) Since it operates in “FIPS140-2 Level 3” mode, it is authorized to generate sets of operator cards and keys. This operation is only required during the key generation ceremony for the CE;j) Request policy approval from the Accreditation Body.
System Administrator	<p>It is responsible for the basic installation and configuration (hardware and software) of the CE up to its initialization. This group must have at least 1 (one) member.</p> <p>The responsibilities of this group are:</p> <ul style="list-style-type: none">a) Install, interconnect and configure the CE's hardware;b) Install and configure the basic software of the CE;c) Keeping an up-to-date inventory of all CE-related products;d) Managing and updating installed products;e) Managing the CAs;

	<p>f) Setting up the necessary initial passwords, which will be changed later by those responsible;</p> <p>g) Prepare announcements on:</p> <ul style="list-style-type: none"> i. The initial passwords; ii. Hash of the installation CD(s) used; iii. The list of all the artifacts (uniquely identified) indispensable for the initialization and operation of the CE.
System Operator	<p>It is responsible for carrying out routine tasks that are essential to the proper functioning and operation of the CE. The responsibilities of this group are:</p> <ul style="list-style-type: none"> a) Manage the Production Environment and the Operating Environment; b) Carrying out the CE's routine tasks, including backing up its systems; c) Carrying out monitoring tasks on the CE systems; d) Monitoring, reporting and quantifying all software and hardware incidents and malfunctions, triggering the appropriate processes to correct them; e) Requesting approval of the forms resulting from the ceremonies from the Management Group for storage in the information environment; f) Taking on the role of System Operator.
Security Officer	<p>It is responsible for proposing all of the CE's policies and ensuring that they are up to date.</p> <p>It is also responsible for the custody of some sensitive artifacts (authentication tokens, etc.), which can be withdrawn by members of the other groups if certain conditions are met. It should be noted that, in order to improve the CE's levels of security, operability and business continuity, there may be several instances of this group, each responsible for the custody of a different set of artifacts. This group should make use of the various secure environments made available for storing this type of item. This group must have a minimum of 2 (two) members.</p>



	<p>The responsibilities of this group are:</p> <ul style="list-style-type: none">a) Manage the Security Administration Environment;b) Define and manage all of the CE's policies and ensure that they are up-to-date and adapted to the reality of the CE;c) Ensure implementation of the defined policies;d) Ensuring that the CE's CPs are supported by the CE's CPS.e) Ensuring that all relevant documents relating directly or indirectly to the operation of the CE and existing in paper format are stored in the Information Environment;f) Explaining all the security mechanisms to employees who need to know them and making them aware of security issues so that they enforce the established security rules and policies.g) Allowing and verifying access to the CE application (groups, rules, logs);h) Checking certificate profiles and end entities in the CE application;i) Verify certificates;j) Activating keys for use. This means that each time the CE is started, the operator cards associated with the keys must be inserted;k) Authorization to generate application keys. This operation is required during the key generation ceremony for the CE;l) Managing the Custody Environment;m) Custody of sensitive artifacts (authentication tokens, etc.) using appropriate means that meet the respective security needs;n) Securely making the artefacts in their custody available to members of other groups who are explicitly authorized to access them, after complying with the appropriate identification and security procedures.
Registry Administration	It is responsible for ensuring that certificates are issued, renewed, suspended and revoked.

	<p>The responsibilities of this group are:</p> <ul style="list-style-type: none"> a) Validate the documentation to be submitted by the holder for issuing/revoking certificates; b) Issuing Certificates if this process is not automated; c) Revoke/Suspend certificates if this process is not automated.
Auditor	<p>The Auditor is authorized to view archives and audit logs. The auditor is also responsible for overseeing internal compliance to determine if NOSICA SSL is operating in accordance with this CP/CPS. This includes acting as internal auditor in NOSICA SSL key ceremonies. A person to whom this role is assigned cannot be a shareholder of CA private keys activation data.</p>

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Handling of CA Private Keys (throughout the entire CA key lifecycle) requires the involvement of at least two trusted persons. Physical and logical access controls exist for the key activation material in order to maintain multi-party and multi-factor control over the Hardware Security Modules containing CA Private Keys.

Shareholders use HSM Smartcard for authentication. The HSM itself enforces dual control based on the HSM smartcards for different functions. The number of needed HSM-smartcards (m) of the total number of produced HSM-smartcards (n) is:

- a) Key generation of Issuing CA = 2 of 6
- b) Signing key activation of Issuing CA = 2 of 6
- c) Private key backup and restore of Issuing CA = 3 of 6.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

All personnel are required to authenticate themselves before they are allowed access to systems necessary to perform their trusted roles.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

No person can have more than two of the roles listed in section 5.2.1 at a time.

To accomplish this separation of duties, NOSICA SSL specifically designates individuals to trusted roles.

NOSICA SSL's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3. PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

NOSICA SSL shall comply with recruitment procedures by assessing the Qualifications, Experience, Clearance and Training of candidates as appropriate for the job function.

Prior to the engagement of any NOSICA SSL employee in the Certificate Management Process, NOSICA SSL verifies the identity and trustworthiness of such person who must be a NOSICA SSL permanent employee. All NOSICA SSL personnel must sign the internal security charter.

Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions. NOSICA SSL personnel have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

5.3.2 BACKGROUND CHECK PROCEDURES

All NOSICA SSL CA personnel are subject to recruitment and selection procedures prior to employment. These procedures undergo background checks, to the extend allowable by law, including, at a minimum:

- criminal records checks,
- employment and education history,

- identity checks using government issued photo ID.

NOSICA SSL personnel do not have access to the trusted functions until all necessary checks are completed and results analyzed. All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are subject to background checks at least every five years.

5.3.3 TRAINING REQUIREMENTS

NOSICA SSL 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.

NOSICA SSL provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this CP/CPS), common threats to the information verification process (including phishing and social engineering), and the CA/B Forum requirements. NOSICA SSL maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

NOSICA SSL documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

NOSICA SSL requires all Validation Specialists to pass an examination provided by NOSICA SSL on the information verification requirements outlined in this CP/CPS.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

All personnel in Trusted Role maintain skill levels consistent with NOSICA SSL's training and performance programs.

Individuals responsible for trusted roles are aware of changes in NOSICA SSL or RA operations, as applicable. Any significant change to the operations has a training plan, and the execution of such plan is documented.

NOSICA SSL provides an information security and privacy training at least once a year to all employees.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

Job rotation of employees is done as necessity arises, depending on the needs of NOSICA SSL, or by request of an individual employee.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

All NOSICA SSL employees are informed that actions that violate the rules established in this CP/DPC, security policy or other rules established by NOSI, EPE, as well as those provided for in applicable national legislation, carry the possibility of disciplinary action in accordance with NOSI, EPE's internal rules and disciplinary procedures in accordance with Cape Verdean Labor Law.

If such violation encompasses a potential criminal offense, NOSICA SSL will report the matter to the appropriate law enforcement agencies for further investigation and action as set forth in Cape Verdean law.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Not Applicable. NOSICA SSL does not support independent contractor requirements.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Personnel are granted access to relevant training documents and governance documents as their intended roles dictate. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.

5.4. AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

NOSICA SSL records events related to the security of its Certificate Systems and Certificate Management Systems. NOSICA SSL records events related to their actions taken to process a Certificate request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate request; the time and date; and the personnel involved. NOSICA SSL makes these records available to its Qualified Auditor. NOSICA SSL records at least the following events:

- a) CA certificate and key lifecycle events, including:
 - 1. Key generation, backup, storage, recovery, archival, and destruction;
 - 2. Certificate requests, renewal, and re-key requests, and revocation;
 - 3. Approval and rejection of certificate requests;
 - 4. Cryptographic device lifecycle management events;
 - 5. Generation of Certificate Revocation Lists;
 - 6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10);
and
 - 7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
- b) Subscriber Certificate lifecycle management events, including:
 - 1. Certificate renewal, and re-key requests, and revocation;
 - 2. All verification activities stipulated in the Baseline Requirements and this CP/CPS;
 - 3. Approval and rejection of Certificate requests;
 - 4. Issuance of Certificates;
 - 5. Generation of Certificate Revocation Lists; and
 - 6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
 - 7. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
 - a) an identifier that uniquely identifies the Network Perspective used;
 - b) the attempted domain name and/or IP address; and

- c) the result of the attempt (e.g., “domain validation pass/fail”, “CAA permission/prohibition”).
- 8. Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request (i.e., “3/4” which should be interpreted as “Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).
- c) Security events, including:
 - 1. Successful and unsuccessful PKI system access attempts;
 - 2. PKI and security system actions performed;
 - 3. Security profile changes;
 - 4. Installation, update and removal of software on a Certificate System;
 - 5. System crashes, hardware failures, and other anomalies;
 - 6. Relevant router and firewall activities (as described in Section 5.4.1.1); and
 - 7. Entries to and exits from the CA facility.

Log records include the following elements:

- Date and time of event;
- The identity of the entity and/or operator that caused the record (when applicable); and
- Description of the event.

All NOSICA SSL CA components are regularly synchronized with a reliable time service. NOSICA SSL CA uses a GPS-NTP time source to establish the correct time for accurate recording of automated log events.

Private keys in any form (e.g., plaintext or enciphered) are never recorded in Audit Logs.

5.4.1.1 ROUTER AND FIREWALL ACTIVITIES LOGS

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.6 MUST at a minimum include:

- 1. Successful and unsuccessful login attempts to routers and firewalls; and

2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 FREQUENCY OF PROCESSING LOG

The logging process allows real-time recording of transactions to identify abnormalities related to failed attempts (access or instruction). In case of manual input, writing is made the same business day as the event. Log events deemed to be security sensitive will automatically generate security incident reports that are handled as defined in section 5.7.

A human review of the logging processes is also performed on application and system logs at least once every 30 days to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log integrity-verification functions are operating properly.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

NOSICA SSL retains for at least 2 years:

- a) CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
 - the destruction of the CA Private Key; or
 - the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key;
- b) Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the expiration of the Subscriber Certificate;
- c) Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

NOSICA SSL makes these audit logs available to its Qualified Auditor upon request.

5.4.4 PROTECTION OF AUDIT LOG

Audit logs are stored in the NOSICA SSL location. Access and security controls are in place to prevent alteration of the audit log. Logical production and archived audit logs are protected through a combination of physical and logical access controls.

All automated logging events are recorded in real time on a secure central logging service in order to prevent log decay or unexpected changes.

5.4.5 AUDIT LOG BACKUP PROCEDURES

For CA components that allow the configuration of multiple logging end-points, automated log events are recorded real-time to central logging services located at NOSICA SSL datacenter.

For CA components that do not support multiple logging end-points, NOSICA SSL makes backup copies of audit logs on a monthly basis according to internal backup procedures. These copies are kept in a safe protected using physical access controls.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

Automated audit data is generated and recorded at the application, network and operating system level. All automated audit logs are sent to a central logging service for collation and review. Manually generated audit data is recorded by NOSICA SSL personnel assigned to Trusted Roles.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

NOSICA SSL is not required to notify a subject that it has been the cause of an auditable event.

5.4.8 VULNERABILITY ASSESSMENTS

NOSICA SSL undergoes a vulnerability scan (i) within one (1) week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that NOSICA SSL determines are significant, and (iii) at least every three (3) months on public and private IP addresses identified as NOSICA SSL's Certificate Systems. NOSICA SSL also undergoes a Penetration Test on Certificate Systems on at least an annual basis and after infrastructure or application upgrades that NOSICA SSL determines are significant.

NOSICA SSL records will be maintained in a manner reasonably sufficient to demonstrate that each Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

NOSICA SSL maintains and implements a formal documented vulnerability management process that includes identification, review, response, and remediation of vulnerabilities as described in Section 6.6.

Additionally, NOSICA SSL performs annual risk assessments that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process;
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that NOSICA SSL has in place to counter such threats.

5.5. RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

NOSICA SSL archives all audit logs (as set forth in Section 5.4.1).

Additionally, NOSICA SSL archives:

- a) Documentation related to the security of its Certificate Systems and Certificate Management Systems;
- b) Documentation related to its verification, issuance, and revocation of certificate requests and Certificates.

NOSICA SSL backs up application, network and system data including:

- Registration information of Subscribers (signed subscriber agreements, IDs of Subscribers, signed Certificate request Forms, proof of legal existence of the organization, etc.),
- Configuration files of NOSICA SSL CA systems,
- All audit logs listed in section 5.4.1,
- Certificate lifecycle information,
- All versions of the CP/CPS and internal documents, including security policies and procedures,
- Ceremony scripts of NOSICA SSL CA key events.

5.5.2 RETENTION PERIOD FOR ARCHIVE

Archived audit logs (as set forth in Section 5.5.1) are retained for a period of at least twenty (20) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, NOSICA SSL retains, for at least twenty (20) years:

- a) All archived documentation related to the security of Certificate Systems and Certificate Management Systems (as set forth in Section 5.5.1); and
- b) All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:



1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
2. the expiration of the Subscriber Certificates relying upon such records and documentation.

5.5.3 PROTECTION OF ARCHIVE

Physical and logical access controls are in place to prevent unauthorized access to archived data in electronic form. Archives are retained and protected against modification or destruction. Only specific NOSICA SSL Trusted Roles, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law.

5.5.4 ARCHIVE BACKUP PROCEDURES

NOSICA SSL maintains and implements backup procedures so that in the event of the loss or destruction of the archives a complete set of backup copies is readily available.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

NOSICA SSL ensures that the precise time of archiving all events, records and documents listed in section 5.4 and 5.5 is recorded. This is accomplished through accurate NTP synchronization of all systems with NOSICA SSL NTP server. Records in paper format have a manually entered date and time.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Archive information is collected internally by NOSICA SSL.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

NOSICA SSL will not divulge archive information to any external party except as follows:

- Where a competent legal authority presents a warrant compelling the release of archived data; or
- Where an audit requires archived data in order to complete a compliance report ;
- Where archived data is electronically generated, the signatures and encryption of this data are checked to ensure its integrity was maintained.

5.6. KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, NOSICA SSL ceases using its expiring CA Private Key to sign Certificates (one year prior to its expiration) and uses the old Private Key only to sign CRLs until the expiry of the last certificate issued under it.

A new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key Certificate is provided to Subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

NOSICA SSL has an Incident Response Procedure and a Disaster Recovery Plan. NOSICA SSL documents a business continuity procedure and disaster recovery plan designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

NOSICA SSL does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity procedure and the risk treatment plan to the NOSICA SSL auditors upon request.

NOSICA SSL annually tests, reviews, and updates these procedures. The business continuity procedure includes:

- a) The conditions for activating the plan,
- b) Emergency procedures,
- c) Fallback procedures,

- d) Resumption procedures,
- e) A maintenance schedule for the plan;
- f) Awareness and education requirements;
- g) The responsibilities of the individuals;
- h) Recovery time objective (RTO);
- i) Regular testing of contingency plans;
- j) NOSICA SSL's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
- k) A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- l) What constitutes an acceptable system outage and recovery time;
- m) How frequently backup copies of essential business information and software are taken;
- n) The distance of recovery facilities to NOSICA SSL main site; and
- o) Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

When NOSICA SSL CA fails to comply with any requirement of this CP/CPS - whether it be a misissuance, a procedural or operational issue, or any other variety of non-compliance - the event is classified as an incident. At a minimum, NOSICA SSL will promptly report all incidents to Mozilla in the form of an Incident Report and will regularly update the Incident Report until the corresponding bug is marked as resolved in the mozilla.org Bugzilla system by a Mozilla representative. NOSICA SSL CA will cease issuance until the problem has been prevented from reoccurring.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

NOSICA SSL CA hosts including Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are built and maintained by a consistent configuration management process. Configuration changes

to these systems are automatically captured and sent to a central monitoring service to determine whether any changes violated the CA's security policies.

If NOSICA SSL determines that such systems have been compromised, NOSICA SSL will investigate the extent of the compromise, and the risk presented to affected parties. NOSICA SSL reserves the right to revoke affected Certificates and to provide new public keys to users.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

In the event that a NOSICA SSL CA private key has been or is suspected to have been compromised, NOSICA SSL personnel will immediately convene an emergency Incident Response Team to assess the situation and to determine the degree and scope of the incident and take appropriate action. The following actions outline as follows:

- Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);
- Begin investigating the incident and determine the degree and scope;
- The Incident Response Team determines the course of action or strategy that should be taken (and in the case of Private Key compromise, determining the scope of Certificates that must be revoked);
- Contact law enforcement, and other interested parties and activate any other appropriate additional security measures;
- Monitor system, continue the investigation, ensure that all data is still being recorded as evidence and make a forensic copy of data collected;
- Isolate, contain and stabilize the system, applying any possible short-term fixes needed to return the system to a normal operating state;
- Prepare an incident report that analyzes the cause of the incident and implement long-term solutions.

A new CA Key Pair should be generated and a new CA Certificate should be signed in accordance with the procedures outlined in Section 6 (Technical Security Controls) of this CP/CPS.

NOSICA SSL will also notify Mozilla and other root stores in the event of a key compromise.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

NOSICA SSL's Disaster Recovery Plan is tested, verified and updated at least annually to be operational in the event of a disaster.

NOSICA SSL systems are configured redundantly on-site and are backed up for failover in the event of a disaster.

5.7.5 MISS-ISSUANCE HANDLING PROCEDURES

In miss-issuance cases, NOSICA SSL will immediately cease issuance from the affected part of NOSICA SSL until the source of the problem has been diagnosed and identified.

Once the problem is diagnosed, NOSICA SSL will put in place at minimum temporary or manual procedures to prevent the problem from re-occurring until a fully automated fix is applied in a reasonable amount of time. NOSICA SSL will restart Certificate issuance after approval of the NOSICA SSL Certificate Policy Authority.

As per Section 4.9.1.1, NOSICA SSL will scan corpus of issued certificates and revoke all certificates found with the same issue.

NOSICA SSL will report the miss-issuance incident to its auditor and to the browser root certificate programs of which NOSICA SSL is a member at the earliest possible date post-incident. The incident report should cover at least the following topics:

- How NOSICA SSL first became aware of the problem (e.g. via a problem report submitted to NOSICA SSL, a notification from the browser root certificate programs of which NOSICA SSL is a member, or internal self-audit), and the time and date.
- A timeline of the actions NOSICA SSL took in response. A timeline is a date-and-time-stamped sequence of all relevant events. This may include events before the incident was reported, such as when a particular requirement became applicable, or a document changed, or a bug was introduced, or an audit was done.
- The date and time NOSICA SSL has stopped issuing certificates with the problem.

- A summary of the problematic Certificates. For each problem: number of Certificates, and the date the first and last Certificates with that problem were issued.
- The complete certificate data for the problematic certificates.
- Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.
- List of steps NOSICA SSL is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when NOSICA SSL expects to accomplish these things and restart Certificate issuance.

5.8. CA OR RA TERMINATION

In case of termination of CA operations for any reason whatsoever, NOSICA SSL will take the following steps prior to the termination:

- Provide subscribers of valid certificates, the operators of the browser root certificate programs and the CA/B Forum with ninety (90) days notice of its intention to cease acting as a CA,
- Revoke 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,
- Destroy all private keys,
- Give timely notice of revocation to each affected Subscriber.

If a successor CA is found which can adopt all of NOSICA SSL responsibilities under its governing documentation, notification to the above shall also be provided explaining this succession. In such a case, the mass revocation may not be warranted.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

6.1.1.1 CA KEY PAIR GENERATION

For the CA Key Pairs, NOSICA SSL performs the following controls:

- a) prepares and follows a Key Generation Script,
- b) has a Qualified Auditor witness the CA Key Pair generation process or records a video of the entire CA Key Pair generation process, and
- c) has a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

In all cases, NOSICA SSL performs the following controls:

- generates the CA key Pair in a physically secured environment as described in section 5.1 of this CP/CPS;
- generates the CA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge as disclosed in section 6.2.1 of this CP/CPS;
- generates the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in section 6.2.2 of this CP/CPS;
- logs its CA Key Pair generation activities and logs all physical access during the key ceremony as disclosed in section 5.4 ; and
- maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in Section 6.2 of this CP/CPS and its Key Generation Script.

6.1.1.2 RA KEY PAIR GENERATION

For the RA Key Pairs, NOSICA SSL performs the following controls:

- a) prepares and follows a Key Generation Script,

- b) has a Internal Auditor witness the RA Key Pair generation process or records a video of the entire RA Key Pair generation process.

In all cases, NOSICA SSL performs the following controls:

- generates the RA key Pair in a physically secured environment as described in section 5.1 of this CP/CPS;
- generates the RA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge as disclosed in section 6.2.1 of this CP/CPS;
- generates the RA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in section 6.2.2 of this CP/CPS;
- logs its RA Key Pair generation activities and logs all physical access during the key ceremony as disclosed in section 5.4 ; and
- maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in Section 6.2 of this CP/CPS and its Key Generation Script.

6.1.1.3 SUBSCRIBER KEY PAIR GENERATION

NOSICA SSL does not generate a Key Pair on behalf of a Subscriber and does not accept a certificate request using a Key Pair previously generated by NOSICA SSL.

NOSICA SSL rejects a Certificate request if one or more of the following conditions are met:

- a) The Key Pair does not meet the requirements set forth in Sections 6.1.5 and/or 6.1.6
- b) There is clear evidence that the specific method used to generate the Private Key was flawed;
- c) NOSICA SSL is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
- d) NOSICA SSL has previously been notified that the Applicant's Private Key has suffered a Key Compromise using NOSICA SSL's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;

e) The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions are to be implemented:

- In the case of Debian weak keys vulnerability (<http://wiki.debian.org/SSLkeys>), NOSICA SSL rejects all keys found at <https://github.com/cabforum/Debian-weak-keys/> for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of 6.1.5, with the exception of RSA key sizes greater than 8192 bits, NOSICA SSL rejects Debian weak keys. see).
- In the case of ROCA vulnerability, NOSICA SSL rejects keys identified by the tools available at <https://github.com/crocs-muni/roca> or equivalent.
- In the case of Close Primes vulnerability (<https://fermatattack.secvuln.info/>), NOSICA SSL rejects weak keys which can be factored within 100 rounds using Fermat's factorization method.

Suggested tools for checking for weak keys can be found here:
<https://cabforum.org/resources/tools/>.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

Applicants are solely responsible for the generation of the private keys used in their Certificate Requests. NOSICA SSL does not provide SSL key generation, escrow, recovery or backup operations.

If NOSICA SSL becomes aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then NOSICA SSL revokes all certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Subscribers generate Key Pairs and submit the Public Key to NOSICA SSL in a CSR as part of the Certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the Certificate.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

NOSICA SSL publishes all CA certificates on its online repository <https://pki.nosi.cv/repositorio>. The browser root certificate programs of which NOSICA SSL is a member will also embed Root Certificate Public Keys into root stores and operating systems.

6.1.5 KEY SIZES

NOSICA SSL uses RSA key pairs and it:

- Ensures that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

NOSICA SSL Certificates meet the following requirements for algorithm type and key size:

6.1.5.2 SUBORDINATE CA CERTIFICATES

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	4096

6.1.5.3 SUBSCRIBER CERTIFICATES

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	2048

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

NOSICA SSL uses a HSM device that conforms to FIPS 186-4 and provides random number generation and onboard generation of up to 4096 bits RSA Public Key. The value of the public exponent is equal to 65537 and the public exponent is in the range between $2^{16} + 1$ and $2^{256} - 1$. The modulus has the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

NOSICA SSL uses CA software that performs quality checks on generated keys for RSA algorithm and also performs regular internal audits against randomly selected samples of Subscriber Certificates per section 8.7.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

NOSICA is a subordinate CA and uses the private keys corresponding to the CA certificates to sign subscriber certificates and certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates).

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

NOSICA SSL implements physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system or device specified in section 6.2.7 consists of physical security and encryption, implemented in a manner that prevents disclosure of the CA Private Key. NOSICA SSL encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

For subscriber keys, NOSICA SSL requires that the private key holder uses reasonable steps to protect the key, such as restrictive permissions and possibly key encryption using a strong passphrase.

6.2.1. CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

The following list shows the requirements for the different users of hardware cryptographic modules are implemented:

- Issuing CAs keys: The HSM used for CA keys meets FIPS 140-2 level 3 requirements ;
- Subscriber keys (SSL Certificate) : The Subscriber is fully responsible for his/her private keys.

A check of the integrity and tests of functionalities of HSMs are done by personnel in trusted roles upon delivery of the HSMs to NOSICA SSL facility. In addition to that, NOSICA SSL maintains controls to provide reasonable assurance that physical access to the HSMs is limited to authorized personnel in trusted roles.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

In all instances, CA private keys are generated in a physically secure environment within cryptographic modules that has been validated to FIPS 140-2 Level-3. CA Certificate signing keys are only used within this secure environment. Access to the modules within the NOSICA SSL environment, including the private keys, is restricted by the use of token/smart cards and associated pass phrases. These smartcards and pass phrases are allocated among multiple Shareholders in trusted roles. Such allocation ensures that no one member of NOSICA SSL personnel in Trusted Roles holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

The following list shows how multi-person controls are implemented:

- Issuing CAs keys: Management access to these keys is only possible using '4-eye' principle (2 out of 4).
- Subscriber keys: The Subscriber has single-person control of the Subscriber keys.

6.2.3 PRIVATE KEY ESCROW

NOSICA SSL does not escrow Private Keys for any reason.

6.2.4 PRIVATE KEY BACKUP

For routine and disaster recovery, NOSICA SSL generates backup copies of CA private keys. The backup, storage, and recovery of these private keys are exclusively performed by personnel holding trusted roles, employing a minimum of dual control in a physically secured environment.

6.2.5 PRIVATE KEY ARCHIVAL

NOSICA SSL does not archive Subscriber Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

NOSICA SSL CA Private Keys are generated, activated and stored in Hardware Security Modules. Private Keys are exported from the HSM only for backup purposes. Private keys are transferred between HSMs according to manufacturers' specifications and only leave the originating device in encrypted form.

When transported between cryptographic modules, the CA encrypts the private key and protects the keys used for encryption from disclosure.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

NOSICA SSL stores Private Keys in cryptographic module that has been validated to FIPS 140-2 Level-3, which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 ACTIVATING PRIVATE KEY

NOSICA SSL is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

The following list shows how private keys are activated:

- Issuing CA keys: The Issuing CA keys are activated with two user keys (physical) and two user PINs (knowledge);
- Subscriber keys: Subscribers are solely responsible for protecting Private Keys in accordance with the obligations that are presented in Subscriber Agreement.

6.2.9 DEACTIVATING PRIVATE KEY

NOSICA SSL deactivates access to its CA Private Keys and stores its cryptographic modules in a secure safe when not in use. NOSICA SSL never leaves its HSM devices in an active unlocked or unattended state.

The method specified in Section 6.2.8 is operated for re-activation of private key.

6.2.10 DESTROYING PRIVATE KEY

NOSICA SSL Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that:

- NOSICA SSL destroys all associated CA secret activation data in such a manner that no information can be used to deduce any part of the Private Key.
- NOSICA SSL initializes the Hardware Security Module according to the specifications of the hardware manufacturer. In cases when this initialization procedure fails, NOSICA SSL will physically destroy the device to remove the ability to extract any private key.

NOSICA SSL does not generate private keys for Subscriber Certificates.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

Public keys, in the form of certificates and certificate requests are archived as per Section 5.5.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The Validity Periods of Certificates issued by NOSICA SSL are as follows:

- The end-user Certificates (SSL Certificates) have a Validity period not greater than 397 days.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day.

6.4. ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

NOSICA SSL activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. Generation and use of CA activation data used to activate CA Private Keys are made during a key ceremony. Activation data is assigned to shareholders in trusted roles as specified in section 5.2.1. The cryptographic hardware is held under multiple person control as explained in Section 5.2.2.

6.4.2 ACTIVATION DATA PROTECTION

NOSICA SSL CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. NOSICA SSL Activation data is protected in cryptographic module that has been validated to FIPS 140-2 Level-3 and may only be used via registered data entry devices.

Repeated attempts to wrongly enter PIN data will cause the activation devices to lock out, and new device issuance to be required.

Subscribers are solely responsible for protecting their private keys activation credentials (PIN, password) and not share them with anyone else.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

NOSICA SSL CA activation data are only held by NOSICA SSL personnel in trusted roles as specified in section 5.2.1.

6.5. COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

NOSICA SSL uses a layered security approach to ensure the security and integrity of the computers used to run the CA software. The following non-exhaustive controls ensure the security of NOSICA SSL operated computer systems:

- Strong identification and authentication for all accounts capable of directly causing Certificate Issuance (physical access control to enter in the room by ID badge and PIN + logic control by certificate to access the system);
- User rights management (to implement the access control policy defined by NOSICA SSL CA, to implement the principles of least privilege, multiple controls and separation of roles);
- Protection against computer viruses and other forms of compromise or unauthorized software and software updates from a trusted software repository;
- Security patches are applied within six (6) months of the security patch's availability, unless NOSICA SSL documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch;
- Manage user accounts, including changes and the rapid removal of access rights;
- Network protection against intrusion of an unauthorized person using the firewall;
- Systems are segmented into networks based on their functional, or logical relationship;
- Networks are configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations;
- Secure and encrypted communication between systems;
- Monitoring and audit procedures of the system configuration, including routing elements, are in place.

6.5.2 COMPUTER SECURITY RATING

NOSICA SSL has established a security framework which covers and governs the technical aspects of its computer security.

As described in section 5.4.8, the systems themselves and the services running on the systems are subject to thorough reviews and testing (including penetration testing). NOSICA SSL operates also a vulnerability management process which includes monitoring of supplier security alerts.

The technical aspects of computer security are subject to periodic audits.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

NOSICA SSL has mechanisms in place to control and monitor the acquisition and development of its CA systems.

Change requests require the approval of the Management Committee. Significant changes require the approval of NOSICA SSL Management Committee. All changes made to the CA systems are logged and tested before deployment.

In this manner, NOSICA SSL can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

All acquisitions made by NOSICA SSL follow the Capeverdean national law. This includes the publication of request for proposals and evaluating each proposal (thus each vendor) according to the set specifications.

All hardware and software are shipped under standard conditions with controls in place to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering. Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors. Updates of equipment or software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

Since NOSICA SSL uses Linting software developed by third parties, it monitors for updated versions of that software and endeavors to plan for updates no later than three (3) months from the release of the update.

NOSICA SSL MAY perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever it updates the Linting software.

6.6.2 SECURITY MANAGEMENT CONTROLS

NOSICA SSL establish formal mechanisms to document, control, monitor, and maintain the security-related configurations and the integrity software, firmware and hardware of its CA systems, including any modifications or upgrades. The NOSICA SSL monitoring control processes includes issuance of alerts automatically and in real time when any changes are detected.

6.6.3 LIFE CYCLE SECURITY CONTROLS

NOSICA SSL applies recommended security patches to Certificate Systems within six months of the security patch's availability, unless it documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

NOSICA SSL does one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by NOSICA SSL vulnerability correction process:

- Remediate the Critical Vulnerability;
- If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to
 - o vulnerabilities with high CVSS scores, starting with the vulnerabilities NOSICA SSL determines are the most critical (such as those with a CVSS score of 10.0), and
 - o systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or
- Document the factual basis for the NOSICA SSL determination that the vulnerability does not require remediation because
 - o NOSICA SSL disagrees with the NVD rating,
 - o the identification is a false positive,

- the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or
- other similar reasons.

6.7. NETWORK SECURITY CONTROLS

NOSICA SSL CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. NOSICA SSL's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses.

NOSICA SSL maintains the Systems in a High Security Zone. NOSICA SSL Keys are kept online to sign Certificate end Entities or periodic CRLs or OCSP Certificates.

Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is NOSICA SSL 's security policy to block all ports and protocols and open only necessary ports to enable CA functions.

All CA equipment is configured with a minimum number of services and accounts and all unused network ports, accounts and services are disabled. All firewall configurations and changes thereto are documented, authorized and implemented in accordance with change management procedures. Changes to network configuration policy go through the same change management process as host devices, and are similarly documented, reviewed and approved.

NOSICA SSL network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

NOSICA SSL implements automated mechanisms under the control of NOSICA SSL trusted roles to process logged system activity and alert multiple destinations of possible Critical Security Events. NOSICA SSL requires trusted role personnel to follow up on alerts of possible Critical Security Events.

6.8. TIME-STAMPING

All NOSICA SSL components are regularly synchronized with a reliable time service. NOSICA SSL uses a GPS-NTP time source to establish the correct time for:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Certificate issued under this CP/CPS conform to the RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1. CERTIFICATE PROFILE

NOSICA SSL meets the technical requirements set forth in Section 2.2 - Publication of Certification Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

NOSICA SSL issues Certificates in accordance with the profiles specified in the Baseline Requirements.

7.1.1 VERSION NUMBER(S)

NOSICA SSL issues X.509 version 3 Certificates.

7.1.2 CERTIFICATE EXTENSIONS

All Certificates that NOSICA SSL issues comply with one of the following certificate profiles described in section 7.1.2 of the Baseline Requirements, which incorporate, and are derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by the Baseline Requirements.

X.509 v3 extensions are supported and used for Certificates profiles as described in Appendix A.

7.1.2.1 ROOT CA CERTIFICATE PROFILE

Not Applicable. NOSICA SSL does not have Root CAs.

7.1.2.1.1 ROOT CA VALIDITY

Not Applicable. NOSICA SSL does not have Root CAs.

7.1.2.1.2 ROOT CA EXTENSIONS

Not Applicable. NOSICA SSL does not have Root CAs.

7.1.2.1.3 ROOT CA AUTHORITY KEY IDENTIFIER

Not Applicable. NOSICA SSL does not have Root CAs.

7.1.2.1.4 ROOT CA BASIC CONSTRAINTS

Not Applicable. NOSICA SSL does not have Root CAs.

7.1.2.2 CROSS-CERTIFIED SUBORDINATE CA CERTIFICATE PROFILE

Not Applicable. NOSICA SSL does not have Cross-Certified Subordinate CAs.

7.1.2.3 TECHNICALLY CONSTRAINED NON-TLS SUBORDINATE CA CERTIFICATE PROFILE

Not applicable. NOSICA SSL does not have a technically constrained non-TLS Subordinate CA in this CA hierarchy.

7.1.2.4 TECHNICALLY CONSTRAINED PRECERTIFICATE SIGNING CA CERTIFICATE PROFILE

Not Applicable. NOSICA SSL does not have a technically constrained precertificate signing CA.

7.1.2.5 TECHNICALLY CONSTRAINED TLS SUBORDINATE CA CERTIFICATE PROFILE

Not Applicable. NOSICA SSL does not issue CAs certificates.

7.1.2.5.1 TECHNICALLY CONSTRAINED TLS SUBORDINATE CA EXTENSIONS

Not Applicable. NOSICA SSL does not issue CAs certificates.

7.1.2.5.2 TECHNICALLY CONSTRAINED TLS SUBORDINATE CA NAME CONSTRAINTS

Not Applicable. NOSICA SSL does not issue CAs certificates.

7.1.2.6 TLS SUBORDINATE CA CERTIFICATE PROFILE

Not Applicable. NOSICA SSL does not issue CAs certificates.

7.1.2.6.1 TLS SUBORDINATE CA EXTENSIONS

Not Applicable. NOSICA SSL does not issue CAs certificates.

7.1.2.7 SUBSCRIBER (SERVER) CERTIFICATE PROFILE

Field	Description
tbsCertificate	
version	MUST be v3 (2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	
notBefore	A value within 48 hours of the certificate signing operation.
notAfter	See Section 6.3.2
subject	See Section 7.1.2.7.1
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.7.6

signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.7.1 SUBSCRIBER CERTIFICATE TYPES

There are four types of Subscriber Certificates that may be issued, which vary based on the amount of Subject Information that is included. Each of these certificate types shares a common profile, with three exceptions: the subject name fields that may occur, how those fields are validated, and the contents of the certificatePolicies extension.

Type	Description
Domain Validated (DV)	See Section 7.1.2.7.2
Individual Validated (IV)	See Section 7.1.2.7.3
Organization Validated (OV)	See Section 7.1.2.7.4
Extended Validation (EV)	Section 7.1.2.7.5

Note: Although each Subscriber Certificate type varies in Subject Information, all Certificates provide the same level of assurance of the device identity (domain name and/or IP address). NOSICA SSL issues OV and DV SSL Certificates with this hierarchy. Refer to Appendix A for NOSICA SSL Subscriber Certificate Profile.

7.1.2.7.2 DOMAIN VALIDATED

For a Subscriber Certificate to be Domain Validated, it MUST meet the following profile:

Field	Requirements
subject	See following table.
certificatePolicies	MUST be present. MUST assert the Reserved Certificate Policy Identifier of 2.23.140.1.2.1 as a policyIdentifier. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All subject names **MUST** be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Domain Validated subject Attributes

Field	Type	Value	Verification
Country (C)	MAY	The two-letter ISO 3166-1 country code for the country associated with the Subject.	Section 3.2.2.3
Common Name (CN)	Not recommended	If present, MUST contain a value derived from the subjectAltName extension according to Section 7.1.4.3.	
Any other attribute	MUST NOT		

7.1.2.7.3 INDIVIDUAL VALIDATED

Not Applicable. NOSICA SSL issues OV and DV SSL Certificates using this hierarchy.

7.1.2.7.4 ORGANIZATION VALIDATED

For a Subscriber Certificate to be Organization Validated, it **MUST** meet the following profile:

Field	Requirements
subject	See following table.
certificatePolicies	MUST be present. MUST assert the Reserved Certificate Policy Identifier of 2.23.140.1.2.2 as a policyIdentifier. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All subject names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Organization Validated subject Attributes

Attribute Name	Presence	Value	Verification
domainComponent	MAY	If present, this field MUST contain a Domain Label from a Domain Name. The domainComponent fields for the Domain Name MUST be in a single ordered sequence containing all Domain Labels from the Domain Name. The Domain Labels MUST be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the Domain Label closest to the root is encoded fir	[Section 3.2]
countryName	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a Country is not represented by an official ISO 3166-1 country code, the CA MUST specify the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	Section 3.2.2.1

stateOrProvinceName	MUST/MAY	MUST be present if localityName is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.	Section 3.2.2.1.
localityName	MUST/MAY	MUST be present if stateOrProvinceName is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.	Section 3.2.2.1
postalCode	NOT RECOMMENDED	If present, MUST contain the Subject's zip or postal information.	Section 3.2.2.1
streetAddress	NOT RECOMMENDED	If present, MUST contain the Subject's street address information. Multiple instances MAY be present	Section 3.2.2.1
organizationName	MUST	The Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY	Section 3.2.2.1

		use "Company Name Inc." or "Company Name". If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.	
surname	MUST NOT	-	-
givenName	MUST NOT	-	-
organizationalUnitName	MUST NOT	-	-
commonName	NOT RECOMMENDED	If present, MUST contain a value derived from the subjectAltName extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.3

Subject attributes don't contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.5 EXTENDED VALIDATION

Not Applicable. NOSICA SSL issues OV and DV SSL Certificates using this hierarchy.

7.1.2.7.6 SUBSCRIBER CERTIFICATE EXTENSION

Extension	Presence	Critical	Description
authorityInformationAccess	MUST	N	See Section 7.1.2.7.7
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
certificatePolicies	MUST	N	See Section 7.1.2.7.9
extKeyUsage	MUST	N	See Section 7.1.2.7.10

subjectAltName	MUST	*	See Section 7.1.2.7.12
nameConstraints	MUST NOT	-	-
keyUsage	SHOULD	Y	See Section 7.1.2.7.11
basicConstraints	MAY	Y	See Section 7.1.2.7.8
crlDistributionPoints	*	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
subjectKeyIdentifier	NOT RECOMMENDED	N	See Section 7.1.2.11.4
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Notes:

- Whether or not the subjectAltName extension should be marked Critical depends on the contents of the Certificate's subject field, as detailed in Section 7.1.2.7.12.
- Whether or not the CRL Distribution Points extension must be present depends on 1) whether the Certificate includes an Authority Information Access extension with an id-ad-ocsp accessMethod and 2) the Certificate's validity period, as detailed in Section 7.1.2.11.2.

7.1.2.7.7 SUBSCRIBER CERTIFICATE AUTHORITY INFORMATION ACCESS

The AuthorityInfoAccessSyntax MUST contain one or more AccessDescriptions. Each AccessDescription MUST only contain a permitted accessMethod, as detailed below, and each accessLocation MUST be encoded as the specified GeneralName type.

The AuthorityInfoAccessSyntax MAY contain multiple AccessDescriptions with the same accessMethod, if permitted for that accessMethod. When multiple AccessDescriptions are present with the same accessMethod, each accessLocation MUST be unique, and

each AccessDescription MUST be ordered in priority for that accessMethod, with the most-preferred accessLocation being the first AccessDescription. No ordering requirements are given for AccessDescriptions that contain different accessMethods, provided that previous requirement is satisfied.

Access Method	OID	Access Location	Presence	Maximum	Description
id-ad-ocs	1.3.6.1.5.5.7.48.1	uniformResourceIdentifier	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
d-ad-calssuers	1.3.6.1.5.5.7.48.2	uniformResourceIdentifier	SHOULD	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	-	MUST NOT	-	No other accessMethods may be used

7.1.2.7.8 SUBSCRIBER CERTIFICATE BASIC CONSTRAINTS

Field	Description
cA	MUST be FALSE
pathLenConstraint	MUST NOT be present

7.1.2.7.9 SUBSCRIBER CERTIFICATE CERTIFICATE POLICIES

If present, the Certificate Policies extension MUST contain at least one PolicyInformation. Each PolicyInformation MUST match the following profile:

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:

A Reserved Certificate Policy Identifier	MUST	The Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1).
anyPolicy	MUST NOT	The anyPolicy Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined and documented in the CA's Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

This Profile RECOMMENDS that the first PolicyInformation value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1). Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.7.10 SUBSCRIBER CERTIFICATE EXTENDED KEY USAGE

Key Purpose	OID	Presence
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST
id-kp-clientAuth	1.3.6.1.5.5.7.3.2	MAY
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	MUST NOT
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	MUST NOT
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	MUST NOT
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.7.11 SUBSCRIBER CERTIFICATE KEY USAGE

The acceptable Key Usage values vary based on whether the Certificate's subjectPublicKeyInfo identifies an RSA public key or an ECC public key. CAs MUST ensure the Key Usage is appropriate for the Certificate Public Key. NOSICA SSL only uses RSA Public Keys in this CA hierarchy.

Key Usage for RSA Public Keys

Key Usage	Permitted	Required
digitalSignature	Y	SHOULD
nonRepudiation	N	-
keyEncipherment	Y	MAY
dataEncipherment	Y	NOT RECOMMENDED
keyAgreement	N	-
keyCertSign	N	-
cRLSign	N	-
encipherOnly	N	-
decipherOnly	N	-

Note: At least one Key Usage MUST be set for RSA Public Keys. The digitalSignature bit is REQUIRED for use with modern protocols, such as TLS 1.3, and secure ciphersuites, while the keyEncipherment bit MAY be asserted to support older protocols, such as TLS 1.2, when using insecure ciphersuites. Subscribers MAY wish to ensure key separation to limit the risk from such legacy protocols, and thus a CA MAY issue a Subscriber certificate that only asserts the keyEncipherment bit. For most Subscribers, the digitalSignature bit is sufficient, while Subscribers that want to mix insecure and secure ciphersuites with the same algorithm may choose to assert both digitalSignature and keyEncipherment within the same certificate, although this is NOT RECOMMENDED. The dataEncipherment bit is currently permitted, although setting it is NOT RECOMMENDED, as it is a Pending Prohibition (<https://github.com/cabforum/servercert/issues/384>). Therefore, NOSICA SSL does not use the dataEncipherment bit.

7.1.2.7.12 SUBSCRIBER CERTIFICATE SUBJECT ALTERNATIVE NAME

For Subscriber Certificates, the Subject Alternative Name MUST be present and MUST contain at least one `dNSName` or `iPAddress` `GeneralName`. See below for further requirements about the permitted fields and their validation requirements.

If the subject field of the certificate is an empty SEQUENCE, this extension MUST be marked critical, as specified in RFC 5280, Section 4.2.1.6. Otherwise, this extension MUST NOT be marked critical.

GeneralName within a subjectAltName extension

Name Type	Permitted	Validation
<code>otherName</code>	N	-
<code>Rfc822Name</code>	N	-
<code>dNSName</code>	Y	The entry MUST contain either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4.

		<p>Wildcard Domain Names MUST be validated for consistency with Section 3.2.2.6. The entry MUST NOT contain an Internal Name. The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry MUST be composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System MUST NOT be included (e.g. "example.com" MUST be encoded as "example.com" and MUST NOT be encoded as "example.com.").</p>
x400Address	N	-
directoryName	N	-
ediPartyName	N	-
uniformResourceIdentifier	N	-
iPAddress	Y	<p>The entry MUST contain the IPv4 or IPv6 address that the CA has confirmed the Applicant controls or has been granted the right to use through a method specified in Section 3.2.2.5. The entry MUST NOT contain a Reserved IP Address.</p>
registeredID	N	-

7.1.2.8 OCSP RESPONDER CERTIFICATE PROFILE

NOSI CA SSL does not directly sign OCSP responses. It uses an OCSP Authorized Responder, as defined by RFC 6960. The OCSP Responder certificate is issued by the same CA that issues the Certificates for which it provides responses.

Refer to Appendix C for NOSICA SSL OCSP responder certificate profile.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.8.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueId	MUST NOT be present
subjectUniqueId	MUST NOT be present
extensions	See Section 7.1.2.8.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.8.1 OCSP RESPONDER VALIDITY

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	The time of signing	Unspecified

7.1.2.8.2 OCSP RESPONDER EXTENSIONS

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1.
extKeyUsage	MUST	-	See Section 7.1.2.8.5
id-pkix-ocsp-nocheck	MUST	N	See Section 7.1.2.8.6
keyUsage	MUST	Y	See Section 7.1.2.8.7
basicConstraints	MAY	Y	See Section 7.1.2.8.4
nameConstraints	MUST NOT	-	-
subjectAltName	MUST NOT	-	-
subjectKeyIdentifier	SHOULD	N	See Section 7.1.2.11.4
authorityInformationAccess	NOT RECOMMENDED	N	See Section 7.1.2.8.3
certificatePolicies	MUST NOT	N	See Section 7.1.2.8.8
crlDistributionPoints	MUST NOT	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.8.3 OCSP RESPONDER AUTHORITY INFORMATION ACCESS

For NOSICA SSL, the extension is NOT USED in OCSP Responder certificates.

7.1.2.8.4 OCSP RESPONDER BASIC CONSTRAINTS

OCSP Responder certificates **MUST NOT** be CA certificates. The issuing CA may indicate this one of two ways: by omission of the basicConstraints extension, or through the inclusion of a basicConstraints extension that sets the cA boolean to FALSE.

Field	Description
cA	MUST be FALSE
pathLenConstraint	MUST NOT be present

Note: Due to DER encoding rules regarding the encoding of DEFAULT values within OPTIONAL fields, a basicConstraints extension that sets the cA boolean to FALSE **MUST** have an extnValue OCTET STRING which is exactly the hex-encoded bytes 3000, the encoded representation of an empty ASN.1 SEQUENCE value.

7.1.2.8.5 OCSP RESPONDER EXTENDED KEY USAGE

Key Purpose	OID	Presence
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST
Any other value	-	MUST NOT

7.1.2.8.6 OCSP RESPONDER ID-PKIX-OCSP-NOCHECK

NOSICA SSL includes the id-pkix-ocsp-nocheck extension (OID: 1.3.6.1.5.5.7.48.1.5). This extension has an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.

7.1.2.8.7 OCSP RESPONDER KEY USAGE

Key Usage	Permitted	Required
digitalSignature	Y	Y
nonRepudiation	N	-
keyEncipherment	N	-

dataEncipherment	N	-
keyAgreement	N	-
keyCertSign	N	-
cRLSign	N	-
encipherOnly	N	-
decipherOnly	N	-

7.1.2.8.8 OCSP RESPONDER CERTIFICATE POLICIES

If present, the Certificate Policies extension MUST contain at least one PolicyInformation. Each PolicyInformation MUST match the following profile:

Permitted policyQualifiers

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	NOT RECOMMENDED	
anyPolicy	NOT RECOMMENDED	
Any other identifier	NOT RECOMMENDED	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

Note: See Section 7.1.2.8.2 for applicable effective dates for when this extension may be included.

Note: Because the Certificate Policies extension may be used to restrict the applicable usages for a Certificate, incorrect policies may result in OCSP Responder Certificates that fail to successfully validate, resulting in invalid OCSP Responses. Including the anyPolicy policy can reduce this risk, but add to client processing complexity and interoperability issues.

7.1.2.9 PRECERTIFICATE PROFILE

A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by the CA that it may issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate.

The CA MAY construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs. The CA MAY use the returned Signed Certificate Timestamps to then alter the Certificate's extensions field, adding a Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3 and as permitted by the relevant profile, prior to signing the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from the CA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the tbsCertificate contents, as transformed by the process defined in RFC 6962, Section 3.2.

This profile describes the transformations that are permitted to a Certificate to construct a Precertificate. NOSICA SSL does not issue a Precertificate unless it is willing to issue a corresponding Certificate, regardless of whether it has done so. Similarly, NOSICA SSL CAs do not issue a Precertificate unless the corresponding Certificate conforms to the Baseline Requirements, regardless of whether NOSICA SSL CAs sign the corresponding Certificate.

A Precertificate is issued directly by NOSICA SSL Issuing CA.

Field	Description
tbsCertificate	
version	Encoded value MUST be byte-for-byte identical to the version field of the Certificate
serialNumber	Encoded value MUST be byte-for-byte identical to the serialNumber field of the Certificate
signature	Encoded value MUST be byte-for-byte identical to the signature field of the Certificate
issuer	Encoded value MUST be byte-for-byte identical to the issuer field of the Certificat
validity	Encoded value MUST be byte-for-byte identical to the validity field of the Certificate

subject	Encoded value MUST be byte-for-byte identical to the subject field of the Certificate
subjectPublicKeyInfo	Encoded value MUST be byte-for-byte identical to the subjectPublicKeyInfo field of the Certificate
issuerUniqueID	Encoded value MUST be byte-for-byte identical to the issuerUniqueID field of the Certificate, or omitted if omitted in the Certificate
subjectUniqueID	Encoded value MUST be byte-for-byte identical to the subjectUniqueID field of the Certificate, or omitted if omitted in the Certificate
extensions	See Section 7.1.2.9.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.9.1 PRECERTIFICATE PROFILE EXTENSIONS - DIRECTLY ISSUED

These extensions apply in the context of a Precertificate directly issued from a CA, and not from a Precertificate Signing CA Certificate, as defined in Section 7.1.2.4.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3
Signed Certificate Timestamp List	MUST NOT	-	
Any other extension	*	*	The order, criticality, and encoded values of all other extensions MUST be byte-for-byte identical to the extensions field of the Certificate

Note: This requirement is expressing that if the Precertificate Poison extension is removed from the Precertificate, and the Signed Certificate Timestamp List is removed from the certificate, the contents of the extensions field MUST be byte-for-byte identical to the Certificate.

7.1.2.9.2 PRECERTIFICATE PROFILE EXTENSIONS - PRECERTIFICATE CA ISSUED

Not Applicable.

7.1.2.9.3 PRECERTIFICATE POISON

The Precertificate MUST contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

This extension MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

7.1.2.9.4 PRECERTIFICATE AUTHORITY KEY IDENTIFIER

Not Applicable. NOSICA SSL does not have a Precertificate Signing CA.

7.1.2.10 COMMON CA FIELDS

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.10.1 CA CERTIFICATE VALIDITY

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.10.2 CA CERTIFICATE NAMING

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.10.3 CA CERTIFICATE AUTHORITY INFORMATION ACCESS

Not Applicable. NOSICA SSL Don't

CAs certificates.

7.1.2.10.4 CA CERTIFICATE BASIC CONSTRAINTS

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.10.5 CA CERTIFICATE CERTIFICATE POLICIES

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.10.6 CA CERTIFICATE EXTENDED KEY USAGE

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.10.7 CA CERTIFICATE KEY USAGE

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.10.8 CA CERTIFICATE NAME CONSTRAINTS

Not Applicable. NOSICA SSL Don't issue CAs certificates.

7.1.2.11 COMMON CERTIFICATE FIELDS

This section contains several fields that are common among multiple certificate profiles. However, these fields may not be common among all certificate profiles. Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.11.1 AUTHORITY KEY IDENTIFIER

Field	Description
-------	-------------

keyIdentifier	MUST be present. MUST be identical to the subjectKeyIdentifier field of the Issuing CA.
authorityCertIssuer	MUST NOT be present
authorityCertSerialNumber	MUST NOT be present

7.1.2.11.2 CRL DISTRIBUTION POINTS

The CRL Distribution Points extension MUST be present in:

- Subordinate CA Certificates; and
- Subscriber Certificates that
 - a) do not qualify as “Short-lived Subscriber Certificates” and
 - b) do not include an Authority Information Access extension with an id-ad-ocsp accessMethod.

The CRL Distribution Points extension SHOULD NOT be present in Root CA Certificates.

The CRL Distribution Points extension is OPTIONAL in Short-lived Subscriber Certificates.

The CRL Distribution Points extension MUST NOT be present in OCSP Responder Certificates.

When present, the CRL Distribution Points extension MUST contain at least one DistributionPoint; containing more than one is NOT RECOMMENDED. All DistributionPoint items must be formatted as follows:

DistributionPoint profile

Field	Presence	Description
distributionPoint	MUST	The DistributionPointName MUST be a fullName formatted as described below.
reasons	MUST NOT	

cRLIssuer	MUST NOT	
-----------	----------	--

A fullName MUST contain at least one GeneralName; it MAY contain more than one. All GeneralNames MUST be of type uniformResourceIdentifier, and the scheme of each MUST be “http”. The first GeneralName must contain the HTTP URL of the Issuing CA’s CRL service for this certificate.

7.1.2.11.3 SIGNED CERTIFICATE TIMESTAMP LIST

If present, the Signed Certificate Timestamp List extension contents MUST be an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in RFC 6962, Section 3.3.

Each SignedCertificateTimestamp included within the SignedCertificateTimestampList MUST be for a PreCert LogEntryType that corresponds to the current certificate.

7.1.2.11.4 SUBJECT KEY IDENTIFIER

If present, the subjectKeyIdentifier MUST be set as defined within RFC 5280, Section 4.2.1.2. The CA MUST generate a subjectKeyIdentifier that is unique within the scope of all Certificates it has issued for each unique public key (the subjectPublicKeyInfo field of the tbsCertificate). For example, CAs may generate the subject key identifier using an algorithm derived from the public key, or may generate a sufficiently-large unique number, such as by using a CSPRNG.

7.1.2.11.5 OTHER EXTENSIONS

All extensions and extension values are not directly addressed by the applicable certificate profile:

- a) MUST apply in the context of the public Internet, unless:
 - the extension OID falls within an OID arc for which the Applicant demonstrates ownership, or,
 - the Applicant can otherwise demonstrate the right to assert the data in a public context.

- b) MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA (such as including an extension that indicates a Private Key is stored on a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).
- c) MUST be DER encoded according to the relevant ASN.1 module defining the extension and extension values.

NOSICA SSL does not include additional extensions or values unless it is aware of a reason for including the data in the certificate.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

All signing algorithms used by NOSICA SSL are sha256WithRSAEncryption. NOSICA SSL CA does not, and never has, used SHA-1 as a component of any signature algorithm on a certificate.

Algorithms OID are conforming to IETF RFC 3279 and RFC 5280.

7.1.3.1 SUBJECTPUBLICKEYINFO

NOSICA SSL indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters are present, and are an explicit NULL.

When encoded, the `AlgorithmIdentifier` for RSA keys is be byte-for-byte identical with the following hexencoded bytes: `300d06092a864886f70d0101010500`.

7.1.3.2 SIGNATURE ALGORITHMIDENTIFIER

All objects signed by a NOSICA SSL CA Private Key MUST conform to the CA/B Forum Baseline Requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

No other encodings are permitted for these fields.

When encoded, the `AlgorithmIdentifier` is byte-for-byte identical with the specified hex-encoded bytes: RSASSA-PKCS1-v1_5 with SHA-256:

`300d06092a864886f70d01010b0500`.

NOSICA SSL does not sign SHA-1 hashes over:

- certificates with an EKU extension containing the id-kp-ocspSigning key purpose;
- “NOSICA SSL Services CA” certificates;
- OCSP responses; or
- CRLs.

7.1.4 NAME FORMS

This section details encoding rules that apply to all Certificates issued by NOSICA SSL. Further restrictions may be specified within Section 7.1.2, but these restrictions do not supersede the Baseline requirements.

7.1.4.1 NAME ENCODING

The following requirements apply to all Certificates listed in Section 7.1.2.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

When encoding a Name, NOSICA SSL ensures that:

- Each Name MUST contain an RDNSequence.
- Each RelativeDistinguishedName MUST contain exactly one AttributeTypeAndValue.
- Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2.

– For example, a RelativeDistinguishedName that contains a countryName AttributeTypeAndValue pair MUST be encoded within the RDNSequence before a RelativeDistinguishedName that contains a stateOrProvinceName AttributeTypeAndValue.

- Each Name MUST NOT contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in these Requirements.

Note: Section 7.1.2.2 provides an exception to the above Name encoding requirements when issuing a CrossCertified Subordinate CA Certificate, as described within that section.

7.1.4.2 SUBJECT ATTRIBUTE ENCODING

The Baseline Requirements document defines requirements for the content and validation of a number of attributes that may appear within the subject field of a tbsCertificate. CAs SHALL NOT include these attributes unless their content has been validated as specified by, and only if permitted by, the relevant certificate profile specified within Section 7.1.2.

CAs that include attributes in the Certificate subject field that are listed in the table below SHALL encode those attributes in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

Encoding and Order Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirement	Max Length
domainComponent	0.9.2342.1920030 0.100.1.25	RFC 4519	MUST use IA5String	63
countryName	2.5.4.6	RFC 5280	MUST use PrintableString	2

stateOrProvinceName	2.5.4.8	RFC 5280	MUST use UTF8String or PrintableString	128
localityName	2.5.4.7	RFC 5280	MUST use UTF8String or PrintableString	128
postalCode	2.5.4.17	X.520	MUST use UTF8String or PrintableString	40
streetAddress	2.5.4.9	X.520	MUST use UTF8String or PrintableString	128
organizationName	2.5.4.10	RFC 5280	MUST use UTF8String or PrintableString	64
surname	2.5.4.4	RFC 5280	MUST use UTF8String or PrintableString	64
givenName	2.5.4.42	RFC 5280	MUST use UTF8String or PrintableString	64
organizationalUnitName	2.5.4.11	RFC 5280	MUST use UTF8String or PrintableString	64
commonName	2.5.4.3	RFC 5280	MUST use UTF8String or PrintableString	64

CAs that include attributes in the Certificate subject field that are listed in the table below SHALL follow the specified encoding requirements for the attribute.

Encoding Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max Length
businessCategory	2.5.4.15	X.520	MUST use UTF8String or PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use PrintableString	2
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use UTF8String or PrintableString	128
jurisdictionLocality	1.3.6.1.4.1.311.60.2.1.1	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use UTF8String or PrintableString	128

serialNumber	2.5.4.5	RFC 5280	MUST use PrintableString	64
organizationIdentifier	2.5.4.97	X.520	MUST use UTF8String or PrintableString	None

7.1.4.3 SUBSCRIBER CERTIFICATE COMMON NAME ATTRIBUTE

If present, this attribute MUST contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2). Since the value of the field is Fully-Qualified Domain Name or Wildcard Domain Name, then it MUST be encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.

7.1.4.4 OTHER SUBJECT ATTRIBUTES

When explicitly stated as permitted by the relevant certificate profile specified within Section 7.1.2, CAs MAY include additional attributes within the AttributeTypeAndValue beyond those specified in Section 7.1.4.2.

Before including such an attribute, NOSICA SSL SHALL:

- Document the attributes within Section 7.1.4 of their CP or CPS, along with the applicable validation practices.
- Ensure that the contents contain information that has been verified by the CA, independent of the Applicant.

7.1.5 NAME CONSTRAINTS

No stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

7.1.6.1 RESERVED CERTIFICATE POLICY IDENTIFIERS

7.1.6.1.1 ROOT CA CERTIFICATES

Not applicable. NOSICA does not operate Root CA.

7.1.6.1.2 SUBORDINATE CA CERTIFICATES

Not applicable. NOSICA SSL does not issue CAs certificates.

7.1.6.1.3 SUBSCRIBER CERTIFICATES

OV SSL certificates must contain the certificate policy identifier 2.23.140.1.2.2, and DV SSL certificates policy identifier 2.23.140.1.2.1.

The certificate policy identifiers of the Subscriber Certificates are listed in the certificate policies extension in Appendix A.

NOSICA SSL asserts that the Certificates issued contain the specified policy identifiers, listed in the certificate policies extension in Appendix A, are managed in accordance with the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

Since the pathLenConstraint is set to zero, no policy constraints were placed on the Issuing CAs.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

NOSICA SSL does not include anything in the Policy Qualifier field of the certificatePolicies extension.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

The certificate policies extension is set to non-critical in NOSICA SSL Subscribers certificates.

7.2. CRL PROFILE

NOSICA SSL issues CRLs in accordance with the profile specified in the current version of the Baseline Requirements.

All CRLs that NOSICA SSL issues comply with the following CRL profile, which incorporates, and is derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 apply, in addition to the normative requirements imposed by the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. NOSICA SSL CRL profiles description is available in Appendix B of this CP/CPS.

A full and complete CRL is a CRL whose scope includes all Certificates issued by the CA.

A partitioned CRL (sometimes referred to as a “sharded CRL”) is a CRL with a constrained scope, such as all Certificates issued by the CA during a certain period of time (“temporal sharding”). Aside from the presence of the Issuing Distribution Point extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile.

NOSICA SSL issues a full and complete CRL and does not issue partitioned CRL nor indirect CRLs (i.e., the issuer of the CRL is not the issuer of all Certificates that are included in the scope of the CRL).

Field	Presence	Description
tbsCertList		
version	MUST	MUST be v2(1), see Section 7.2.1
signature	MUST	See Section 7.1.3.2
issuer	MUST	MUST be byte-for-byte identical to the subject field of the Issuing CA.
thisUpdate	MUST	Indicates the issue date of the CRL.

nextUpdate	MUST	Indicates the date by which the next CRL will be issued. For CRLs covering Subscriber Certificates, at most 10 days after the thisUpdate. For other CRLs, at most 12 months after the thisUpdate.
revokedCertificates	*	been revoked and the corresponding entry has yet to appear on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. The CA SHOULD remove an entry for a corresponding Certificate after it has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. See the "revokedCertificates Component" table for additional requirements.
extensions	MUST	See the "CRL Extensions" table for additional requirements.
signatureAlgorithm	MUST	Encoded value MUST be byte-for-byte identical to the tbsCertList.signatur
signature	MUST	-
Any other value	NOT RECOMMENDED	-

7.2.1 VERSION NUMBER(S)

NOSICA SSL issues X.509 Version 2 CRLs in accordance with IETF PKIX RFC 5280.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

CRL Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
CRLNumber	MUST	N	MUST contain an INTEGER greater than or equal to zero (0) and less than 2^{159} , and convey a strictly increasing sequence.
IssuingDistributionPoint	*	Y	See Section 7.2.2.1 CRL Issuing Distribution Point
Any other extension	NOT RECOMMENDED	-	-

revokedCertificates Component

Component	Presence	Description
serialNumber	MUST	MUST be byte-for-byte identical to the serialNumber contained in the revoked Certificate.
revocationDate	MUST	Normally, the date and time revocation occurred. See the footnote following this table for circumstances where backdating is permitted.
crEntryExtensions	*	See the “crEntryExtensions Component” table for additional requirements.

Note: NOSICA SSL will update the revocation date in a CRL entry when it is determined that the private key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate. Backdating the revocationDate field is an exception to best practice described in RFC 5280 (Section 5.3.2); however, these

requirements specify the use of the revocationDate field to support TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

crlEntryExtensions Component

CRL Entry Extension	Presence	Description
reasonCode	*	When present (OID 2.5.29.21), MUST NOT be marked critical and MUST indicate the most appropriate reason for revocation of the Certificate. MUST be present unless the CRL entry is for a Certificate not technically capable of causing issuance and either 1) the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023 or 2) the reason for revocation (i.e., reasonCode) is unspecified (0). See the “CRLReasons” table for additional requirements.
Any other value	NOT RECOMMENDED	-

CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
unspecified	0	Represented by the omission of a reasonCode. MUST be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023.
keyCompromise	1	Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
affiliationChanged	3	Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
superseded	4	Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with these Baseline Requirements or the CA's CP or CPS.

cessationOfOperation	5	Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.
certificateHold	6	MUST NOT be included if the CRL entry is for 1) a Certificate subject to these Requirements, or 2) a Certificate not subject to these Requirements and was either A) issued on-or-after 2020- 09-30 or B) has a notBefore on-or-after 2020-09-30.
privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The Subscriber Agreement, and any online resource referenced therein, informs Subscribers about the revocation reason options listed above and provides explanation about when to choose each option. The tools that NOSICA SSL provides to the Subscriber allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL).

The privilegeWithdrawn reasonCode is not made available to the Subscriber as a revocation reason option, because the use of this reasonCode is determined by NOSICA SSL and not the Subscriber.

When NOSICA SSL obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode

extension with a non-keyCompromise reason, NOSICA SSL will update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension when this is technically possible.

7.2.2.1 CRL ISSUING DISTRIBUTION POINT

NOSICA SSL does not issue partitioned CRLs.

NOSICA SSL does not assert both of the onlyContainsUserCerts and onlyContainsCACerts fields. The indirectCRL and onlyContainsAttributeCerts fields are set to FALSE (i.e., not asserted).

The onlySomeReasons field is not included; as NOSICA SSL issues full and complete CRLs.

7.3. OCSP PROFILE

The NOSICA SSL OCSP functionality is built according to RFC 6960.

The NOSICA SSL provides uninterrupted on-line Certificate status protocol OCSP support which is a real time Certificate status inquiry. By this service, when appropriate Certificate status inquiries are received, the status of Certificates and additional information as required by the protocol are returned to the inquirer as the response.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 VERSION NUMBER

The OCSP service provided by NOSICA SSL supports the v1 protocol version under the “IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP” document.

7.3.2 OCSP EXTENSIONS

NOSICA SSL OCSP responder certificate profile description is available in Appendix C of this CP/CPS.

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

NOSICA SSL is an entity licensed under Cape Verdean law to act as a Certification Authority. NOSICA SSL shall at all times act in accordance with the following:

- a) the requirements of this CP/CPS;
- b) the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates of the CA/B Forum; and
- c) the latest versions of the WebTrust Principles and Criteria For Certification Authorities – SSL Baseline With Network Security and the WebTrust Principles And Criteria For Certification Authorities.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

NOSICA SSL is subject to a full audit, as specified in section 8 of this CP/PPC.

An annual audit is performed by an independent external auditor to assess NOSICA SSL's compliance with requirements set forth above.

An audit period must not exceed one year in duration. In addition to that, more than one compliance audit per year is possible if this is requested by NOSICA SSL or is a result of unsatisfactory results of a previous audit.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

NOSICA SSL's 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:

- a) Independence from the subject of the audit;

- b) The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1 of the CA/B Forum Baseline Requirements);
- c) For audits conducted in accordance with the WebTrust standard licensed by WebTrust;
- d) For audits conducted in accordance with any one of the ETSI standards accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
- e) Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the thirdparty attestation function; and
- f) Bound by law, government regulation, or professional code of ethics.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

NOSICA SSL utilizes independent auditors that do not have any financial interest or business relationship that could foreseeably create a significant bias for or against NOSICA SSL.

8.4. TOPICS COVERED BY ASSESSMENT

NOSICA SSL undergoes an audit in accordance with:

“Principles and Criteria for Certification Authorities” Version 2.2 or newer; and either “WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security” Version 2.7 or newer; or

“WebTrust Principles and Criteria for Certification Authorities – SSL Baseline” Version 2.8 or newer and “WebTrust Principles and Criteria for Certification Authorities – Network Security” Version 1.7 or newer.

Topics covered in this annual audit include, but are not limited to, the requirements of this CP/CPS, environmental controls, CA key management, and certificate life cycle management.

The chosen audit scheme incorporates periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit is conducted by a Qualified Auditor, as specified in Section 8.2.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

With respect to compliance audits of NOSICA SSL's operations, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by NOSICA SSL Management Committee with input from the auditor. If exceptions or deficiencies are identified, NOSICA SSL management is responsible for developing and implementing a corrective action plan. Once the plan has been implemented, NOSICA SSL will call for an auxiliary audit to verify that the noted deficiencies have been remediated.

if the deficiency is deemed so serious, or the time to remediate so long as to call into question the integrity of certificates issued, NOSICA SSL will inform the relevant browser root certificate program managers that a serious deficiency in practice has been uncovered, and that they should take such steps as to mitigate the risk to their program's integrity.

8.6. COMMUNICATION OF RESULTS

NOSICA SSL makes the Audit Report publicly available at <https://pki.nosi.cv/repositorio>. The results will also be sent to any other appropriate entities that may be entitled by law, regulation, or agreement to receive a copy of the audit results. Such parties include the relevant browser root certificate program managers.

NOSICA SSL makes its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, NOSICA SSL will provide an explanatory letter signed by the Qualified Auditor.

The Audit Report contains at least the following clearly-labeled information:

- a) name of the organization being audited;
- b) name and address of the organization performing the audit;
- c) the SHA-256 fingerprint of all Subordinate CA Certificates, that were in-scope of the audit;
- d) audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
- e) a list of the CA policy documents, with version numbers, referenced during the audit;
- f) whether the audit assessed a period of time or a point in time;
- g) the start date and end date of the Audit Period, for those that cover a period of time;
- h) the point in time date, for those that are for a point in time;
- i) the date the report was issued, which will necessarily be after the end date or point in time date.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and NOSICA SSL will ensure it is publicly available.

The Audit Report MUST be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7. SELF-AUDITS

NOSICA SSL performs regular internal audits of its operations, personnel, and compliance with this CP/CPS.

During the period in which NOSICA SSL issues Certificates, NOSICA SSL monitors adherence to this CP/CPS and the CA/B Forum Baseline Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the

Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

NOSICA SSL uses a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

NOSICA SSL charges fees for issuing of Certificates according to the respective price list published on their website <https://pki.nosi.cv/> or made available upon request.

The update of the fees goes through the Board of Directors of NOSICA SSL.

9.1.2 CERTIFICATE ACCESS FEES

NOSICA SSL does not charge fees for access to its Certificate databases.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

NOSICA SSL does not charge a Certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL or the OCSP.

9.1.4 FEES FOR OTHER SERVICES

NOSICA SSL may elect to charge fees for its other services. Such fees will be outlined in the applicable Subscriber agreement.

9.1.5 REFUND POLICY

NOSICA SSL does not refund the fees of Certificates.



9.2. FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

NOSICA SSL currently maintains a commercial general liability insurance according to the National Law.

9.2.2 OTHER ASSETS

Not applicable.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No warranty coverage is available for Subscribers and Relying Parties except the warranties listed in section 9.6.1.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

NOSICA SSL keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel. Confidential information includes, but is not limited to:

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Disaster Recovery, and Business Continuity Plans ;
- Any certificate application records and documentation submitted in support of certificate applications, which is not in relation to an issued certificate, whether successful or rejected ;
- External or internal audit trail records and reports, which are not required to be openly published ;
- Transaction records, financial audit records, and internal records on the operations of NOSICA SSL's infrastructure, certificate management, services and data.



9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

The following are not considered confidential:

- Certificates;
- Certificate revocation Lists;
- CP/CPS; and
- any information available in NOSICA SSL repository at <https://pki.nosi.cv/repositorio>.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

NOSICA SSL protects and secures confidential information from disclosure. All employees of NOSICA SSL are bound by NOSICA SSL Information Security Policy and required by the security chart engagements to preserve the confidentiality of information so labeled.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

NOSICA SSL protects personal information in accordance with the Capeverdean law N° 121/IX/2021, of March 17th, on the protection of personal data and NOSICA SSL internal document.

NOSICA SSL makes available to Subscribers and Relying Parties the company Privacy Policy on the website <https://pki.nosi.cv/repositorio>.

9.4.2 INFORMATION TREATED AS PRIVATE

NOSICA SSL treats all personal information about an individual that is not publicly available in the contents of a Certificate, CRL or OCSP as private information. NOSICA SSL protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Private information does not include Certificates, CRLs, and the personal or corporate information appearing in them.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

NOSICA SSL employees and contractors are expected to handle personal information in strict confidence and meet the requirements of Cabo Verde law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

Personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. As part of a Subscriber Agreement, all Subscribers consent to the global transfer of any personal data contained in the Certificate and agree to allow NOSICA SSL to handle any private information required for the issuance and maintenance of certificates.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

NOSICA SSL will only release or disclose private information on judicial or other authoritative order.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

NOSICA SSL is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by a legal entity as stated in section 9.4.6.

9.5. INTELLECTUAL PROPERTY RIGHTS

NOSICA SSL does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them.

NOSICA SSL owns the intellectual property rights in NOSICA SSL's services, including the certificates, trademarks used in providing the services, and this CP/CPS. Certificate and revocation information are the property of NOSICA SSL.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

By issuing a Certificate, NOSICA SSL makes the Certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement;
- All Application Software Suppliers with whom NOSICA SSL has entered into a contract for inclusion of its Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a Valid Certificate.

NOSICA SSL represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, NOSICA SSL has complied with the CA/B Forum Baseline Requirements and this CP/CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

- a) **Right to Use Domain Name:** That, at the time of issuance, NOSICA SSL (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
- b) **Authorization for Certificate:** That, at the time of issuance, NOSICA SSL (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the

Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;

- c) **Accuracy of Information:** That, at the time of issuance, NOSICA SSL (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
- d) **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, NOSICA SSL implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 7.1.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
- e) **Subscriber Agreement:** That, if NOSICA SSL and the Subscriber are not Affiliated, the Subscriber and NOSICA SSL are parties to a legally valid and enforceable Subscriber Agreement that satisfies the CA/B Forum Baseline Requirements, or, if NOSICA SSL and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- f) **Status:** That NOSICA SSL maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- g) **Revocation:** That NOSICA SSL will revoke the Certificate for any of the reasons specified in the CA/B Forum Baseline Requirements.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

NOSICA SSL RA represents that:

- Information provided by NOSICA SSL RA does not contain any false or misleading information, and
- All Certificates requested by NOSICA SSL RA meet the requirements of the applicable CP/CPS.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

NOSICA SSL requires, as part of the Subscriber Agreement, that the Applicant makes the commitments and warranties in this section for the benefit of NOSICA SSL and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, NOSICA SSL obtains, for the express benefit of NOSICA SSL and the Certificate Beneficiaries, the Applicant's agreement to the Subscriber Agreement with NOSICA SSL CA.

NOSICA SSL implements a process to ensure that each Subscriber Agreement is legally enforceable against the Applicant. In either case, the Agreement is applied to the Certificate to be issued pursuant to the Certificate request.

A separate Agreement is used for each Certificate request, or a single Agreement is used to cover multiple future Certificate requests and the resulting Certificates, so long as each Certificate that NOSICA SSL issues to the Applicant is clearly covered by that Subscriber Agreement.

The Subscriber Agreement contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- a) **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to NOSICA SSL, both in the Certificate request and as otherwise requested by NOSICA SSL in connection with the issuance of the Certificate(s) to be supplied by NOSICA SSL;
- b) **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- c) **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- d) **Use of Certificate:** An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;
- e) **Reporting and Revocation:** An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if



there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

- f) **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise;
- g) **Responsiveness:** An obligation to respond to NOSICA SSL's instructions concerning Key Compromise or Certificate misuse within a specified time period;
- h) **Acknowledgment and Acceptance:** An acknowledgment and acceptance that NOSICA SSL is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by the present CP/CPS, or the CA/B Forum Baseline Requirements.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

Each Relying Party represents that, prior to relying on a NOSICA SSL Certificate, it:

- Obtained sufficient knowledge on the use of digital Certificates and PKI,
- Studied the applicable limitations on the usage of Certificates and agrees to NOSICA SSL's limitations on liability related to the use of Certificates,
- Has read, understands, and agrees to this CP/CPS,
- Verified both the NOSICA SSL Certificate and the Certificates in the Certificate chain using the relevant CRL or OCSP,
- Will not use a NOSICA SSL Certificate if the Certificate has expired or been revoked, and
- Will take all reasonable steps to minimize the risk associated with relying on a NOSICA SSL Certificate after considering:
 - applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction,
 - the intended use of the Certificate as listed in the Certificate or this CP/CPS,

- the data listed in the Certificate,
- the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
- the Relying Party's previous course of dealing with the Subscriber,
- the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
- any other indication of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No implied or express warranties are given by NOSICA SSL to other participants other than in Subscriber agreements, Relying Party agreements and any other agreements signed by NOSICA SSL with Third Parties.

9.7. DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, this CP/CPS, the Subscriber Agreement, and any other contractual agreement applicable within the NOSICA SSL PKI shall disclaim NOSICA SSL possible warranties, including any warranty of merchantability or fitness for a particular purpose.

To the extent permitted by applicable law, NOSICA SSL makes no express or implied representations or warranties pursuant to this CP/CPS. NOSICA SSL expressly disclaims any and all express or implied warranties of any type to any person, including any implied warranty of title, non-infringement, merchantability, or fitness for a particular purpose.

9.8. LIMITATIONS OF LIABILITY

NOSICA SSL is only liable for damages which are the result of its failure to comply with this CP/CPS and which were provoked deliberately or wantonly negligent.

NOSICA SSL is not in any event liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. NOSICA SSL is not liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions.

NOSICA SSL is not in any event liable for damages that result from force major events as detailed in section 9.15. NOSICA SSL takes commercially reasonable measures to mitigate the effects of force major in due time. Any damages resulting of any delay caused by force major will not be covered by NOSICA SSL. The Subscriber is liable to NOSICA SSL and Relying Parties for any damages resulting from misuse, willful misconduct, failure to meet regulatory obligations, or noncompliance with other provisions for using the Certificate.

9.9. INDEMNITIES

9.9.1 INDEMNIFICATION BY NOSICA SSL

Notwithstanding any limitations on its liability to Subscriber and Relying Parties, NOSICA SSL acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with NOSICA SSL do not assume any obligation or potential liability of NOSICA SSL under this CP/CPs or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. NOSICA SSL shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by NOSICA SSL, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by NOSICA SSL where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available

from NOSICA SSL online, and the application software either failed to check such status or ignored an indication of revoked status).

Additional indemnity provisions and obligations are contained within relevant contractual agreements such as the Subscriber Agreement.

9.9.2 INDEMNIFICATION BY SUBSCRIBERS

To the extent permitted by law, each Subscriber shall release, indemnify and hold harmless NOSICA SSL, and all NOSICA SSL directors, shareholders, officers, agents, employees, contractors and successors of the foregoing, against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of its Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of a certificate or Private Key.

9.9.3 INDEMNIFICATION BY RELYING PARTIES

To the extent permitted by law, each Relying Party shall release, indemnify and hold harmless NOSICA SSL, and all NOSICA SSL directors, shareholders, officers, agents, employees, contractors and successors of the foregoing against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by NOSICA SSL or its affiliates and used by the Relying Party, this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10. TERM AND TERMINATION

9.10.1 TERM

This CP/CPS and any amendments thereto, are effective upon publication in NOSICA SSL's Repository.

9.10.2 TERMINATION

This CP/CPS, as may be amended from time to time, is effective until replaced by a new version, which shall be published in NOSICA SSL's Repository.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon Termination of this CP/CPS, Subscribers, and Relying Parties are bound by its terms for all Certificates issued, while it's effective, for the remainder of the validity periods of such Certificates.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

NOSICA SSL, Subscribers, Applicants, Relying Parties and other participants will use official means of communication as per Cabo Verde National Law.

9.12. AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

This CP/CPS is reviewed at least annually and may be reviewed more frequently. Revisions of this CP/CPS are reviewed and approved within NOSICA SSL Management Committee. Amendments are made by posting an updated version of the CP/CPS to the online repository. Changes to this CP/CPS are indicated by an incremental version number.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

Updates, amendments, and new versions of NOSICA SSL's CP/CPS shall be posted in NOSICA SSL's repository. Such publication shall serve as notice to all relevant entities.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

If NOSICA SSL's Management Committee determines that a change is necessary in the object identifier corresponding to this CP/CPS, the amendment shall contain new object identifiers for this CP/CPS. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13. DISPUTE RESOLUTION PROVISIONS

Parties are required to notify NOSICA SSL and attempt to resolve disputes directly with NOSICA SSL before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. GOVERNING LAW

This CP/CPS is governed, construed and interpreted in accordance with the laws of Cabo Verde. The law of Cabo Verde applies also to all NOSICA SSL commercial or contractual relationships in which this CP/CPS may apply or quoted implicitly or explicitly in relation to NOSICA SSL products and services where NOSICA SSL acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including NOSICA SSL partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Praia in Cabo Verde.

9.15. COMPLIANCE WITH APPLICABLE LAW

NOSICA SSL issues Certificates and operate its PKI in accordance with Capeverdean law.

9.16. MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

This CP/CPS and the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and NOSICA SSL and shall supersede any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CP/CPS and any other express agreement between a Subscriber or Relying Party with NOSICA SSL with

respect to a Certificate, including but not limited to a Subscriber Agreement or the Relying Party Agreement shall take precedence.

9.16.2 ASSIGNMENT

Entities operating under this CP/CPS cannot assign their rights or obligations without the prior written consent of NOSICA SSL.

9.16.3 SEVERABILITY

In the event of a conflict between the CA/B Forum Baseline Requirements and a Capeverdean law, regulation or government order, NOSICA SSL may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Cabo Verde.

This applies only to operations or certificate issuances that are subject to that Law. In such event, NOSICA SSL will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the CA/B Forum Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by NOSICA SSL.

NOSICA SSL will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at <https://cabforum.org/pipermail/public/> (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to NOSICA SSL practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP/CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

NOSICA SSL may seek indemnification and any fees (including reasonable attorney's fees and court costs) from a party for damages, losses and expenses related to that party's conduct.

NOSICA SSL's failure to enforce a provision of this CP/CPS does not waive NOSICA SSL's right to enforce the same provision later, or right to enforce any other provision of this CP/CP.

9.16.5 FORCE MAJEURE

NOSICA SSL is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond NOSICA SSL's reasonable control. The operation of the Internet is beyond NOSICA SSL's reasonable control.

9.17. OTHER PROVISIONS

The present CP/CPS does not state any conditions in this respect.

APPENDIX A: NOSICA SSL PKI END-ENTITY PROFILE

The following tables provides the description of the fields for NOSICA SSL Certificates issued under **NOSICA SSL**:

Organization Validated – SSL Subscriber Certificate

Base Profile	Included	Critical	O/M ¹	CO ²	Values
Data:					
Version	X	False	M	S	3 (0x2)
Serial Number	X	False	M	FDV	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
Signature Algorithm	X	False	M	S	SHA256 with RSA Encryption
Issuer	X	False	M	S	CN=NOSICA-SSL OU=NOSI-Nucleo Operacional da Sociedade de Informacao O=ICP-CV C=CV
Validity					
Not Before	X	False	M	D	Certificate generation process date/time
Not After	X	False	M	D	Certificate generation process date/time + 365 days.
Subject					
C, countryName	X	False	M	D	The two-letter ISO 3166-1 country code for the country associated with the Subject
L, localityName	X	False	M	D	Location in which the company's registered office is established.
O, OrganizationName	X	False	M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.

1. O/M: O = Optional, M = Mandatory.

2. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA

CN, commonName	X	False	O	D	If present, this field contains exactly one entry that is one of the values contained in the Certificate's 'subjectAltName' extension (see Section 7.1.4.3 of the Baseline Requirements). Since the value of this field is a Fully-Qualified Domain Name or Wildcard Domain Name, then this value MUST be encoded as a character-for-character copy of the 'dNSName' entry value from the 'subjectAltName' extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.
Subject Public Key Info:					
Public Key Algorithm	X	False	M	S	rsaEncryption
RSA Public Key	X	False	M	S	(2048 bit)
Modulus (2048 bit)	X	False	M	S	
Exponent	X	False	M	S	65537 (0x10001)
X509v3 extensions					
Authority Information Access	X	False	M	S	CA - ISSUERS – URI : https://pki.nosi.cv/nosica-ssl.der OCSP - URI : https://ocsp.nosi.cv
X509v3 Subject Key Identifier:	X	False	M	D	assigned by CA to each certificate
X509v3 Basic Constraints:	X	True	M	S	CA:False
X509v3 Authority Key Identifier	X	False	M	S	NOSICA SSL key Identifier
X509v3 Certificate Policies	X	False	M	S	Policy: 2.23.140.1.2.2 Policy : 0.4.0.2042.1.7 Policy: 2.16.132.1.2.2.6 URI: https://pki.nosi.cv/cp_cps_nosica-ssl.pdf

					Policy: 2.16.132.1.3.2.6 URI: https://pki.nosi.cv/cp_cps_nosica-ssl.pdf
X509v3 CRL Distribution Points	X	False	M	S	URI: https://pki.nosi.cv/nosica-ssl.crl
X506v3 Key Usage	X	True	M	S	Digital Signature, Key Encipherment
X509v3 Extended Key Usage	X	False	M	S	TLS Web Client Authentication, TLS Web Server Authentication
X509v3 Subject alternative Name	X	False	M	D	DNS: FQDN (Fully-Qualified Domain Name) of application/server.

1. O/M: O = Optional, M = Mandatory.

2. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA

Domain Validated – SSL Subscriber Certificate

Base Profile	Included	Critical	O/M ₁	CO ²	Values
Data:					
Version	X	False	M	S	3 (0x2)
Serial Number	X	False	M	FDV	A non-sequential number greater than zero (0) and less than 2 ¹⁵⁹ containing at least 64 bits of output from a CSPRNG.
Signature Algorithm	X	False	M	S	SHA256 with RSA Encryption
Issuer	X	False	M	S	CN=NOSICA-SSL OU=NOSI-Nucleo Operacional da Sociedade de Informacao O=ICP-CV C=CV
Validity					
Not Before	X	False	M	D	Certificate generation process date/time
Not After	X	False	M	D	Certificate generation process date/time + 365 days.
Subject					
C, countryName	X	False	O	D	The two-letter ISO 3166-1 country code for the country associated with the Subject

CN, commonName	X	False	O	DV	If present, this field contains exactly one entry that is one of the values contained in the Certificate's 'subjectAltName' extension (see Section 7.1.4.2.1 of the Baseline Requirements). Since the value of this field is a Fully-Qualified Domain Name or Wildcard Domain Name, then this value MUST be encoded as a character-for-character copy of the 'dNSName' entry value from the 'subjectAltName' extension. Specifically, all Domain Labels of the Fully- Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.
Subject Public Key Info:					
Public Key Algorithm	X	False	M	S	rsaEncryption
RSA Public Key	X	False	M	S	(2048 bit)
Modulus (2048 bit)	X	False	M	S	
Exponent	X	False	M	S	65537 (0x10001)
X509v3 extensions					
Authority Information Access	X	False	M	S	CA - ISSUERS – URI : https://pki.nosi.cv/nosica-ssl.der OCSP - URI : https://ocsp.nosi.cv
X509v3 Subject Key Identifier:	X	False	M	D	This extension identifies the public key being certified.
X509v3 Basic Constraints:	X	True	M	S	CA: False
X509v3 Authority Key Identifier	X	False	M	S	NOSICA SSL key Identifier
X509v3 Certificate Policies	X	False	M	S	Policy: 2.23.140.1.2.1 Policy: 0.4.0.2042.1.7 Policy: 2.16.132.1.2.2.6 Policy: 2.16.132.1.3.2.6
X509v3 CRL Distribution	X	False	M	S	URI: https://pki.nosi.cv/nosica-ssl.crl



Points					
X506v3 Key Usage	X	True	M	S	Digital Signature, Key Encipherment
X509v3 Extended Key Usage	X	False	M	S	TLS Web Client Authentication, TLS Web Server Authentication
X509v3 Subject alternative Name	X	False	M	D	The entry contains either a Fully-Qualified Domain Name or Wildcard Domain Name that NOSICA SSL has validated in accordance with Section 3.2.2.4 . Wildcard Domain Names are validated for consistency with Section 3.2.2.6 . The entry does not contain an Internal Name. The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry is be composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System is not included

1. O/M: O = Optional, M = Mandatory.

2. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA

APPENDIX B: PROFILE OF THE CRL OF NOSICA SSL

The following table describes the CRL profile of NOSICA SSL:

Field	Presence	Critical	Value
tbsCertlist			
Version	MUST		2 (0x1)
Signature	MUST		RSASignature
Issuer	MUST		CN=NOSICA-SSL OU=NOSI-Nucleo Operacional da Sociedade de Informacao O=ICP-CV C=CV
ThisUpdate	MUST		CRL generation process date/time.
NextUpdate	MUST		CRL generation process date/time + 7 days
CRL extensions	MUST		
Authority Key Identifier	MUST	N	NOSICA SSL key Identifier
CRL Number	MUST	N	A monotonically increasing sequence number
Revoked Certificates:			
Serial Number	MUST		Serial number of the revoked certificate
Revocation Date	MUST		Date and time of the revocation
CRL entry extensions:			
CRL Reason Code	MUST		Code of Reason of revocation
Signature Algorithm	MUST		sha256WithRSASignature
Signature	MUST		

APPENDIX D: OCSP RESPONDER CERTIFICATE PROFILE

The following table describes the OCSP profile of NOSICA SSL:

Field	Presence	Critical	Value
tbsCertlist			
Version	MUST		V3 (2)
SerialNumber	MUST		A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
Signature	MUST		RSASignature
Issuer	MUST		CN=NOSICA-SSL OU=NOSI-Nucleo Operacional da Sociedade de Informacao O=ICP-CV C=CV
Validity	MUST		
notBefore	MUST		Minimum: One day prior to the time of signing Maximum: The time of signing
notAfter	MUST		Minimum: The time of signing Maximum: 365 days
Subject	MUST		
countryName	MUST		CV
organizationName	MUST		ICP-CV
organizationalUnitName	MUST		NOSI-Nucleo Operacional da Sociedade de Informacao
commonName	MUST		OCSPResponder_NOSICA-SSL
SubjectPublicKeyInfo	MUST		RSA Encryption
Extensions	MUST		
Authority Key Identifier		N	
keyIdentifier	MUST	N	NOSICA SSL subject key Identifier
extKeyUsage		-	
id-kp-OCSPSigning	MUST	-	OID: 1.3.6.1.5.5.7.3.9
id-pkix-ocsp-nocheck	MUST	N	OID: 1.3.6.1.5.5.7.48.1.5
keyUsage	MUST	Y	
digitalSignature	MUST	Y	Permitted: Y Required : Y
basicConstraints	MAY	Y	cA : FALSE
subjectKeyIdentifier	SHOULD	N	assigned by CA to each certificate
Signed Certificate Timestamp List	MAY	N	Provided by CA
Signature Algorithm	MUST		tbsCertificate.signature
Signature			