Greek Universities Network (GUnet)

Hellenic Academic and Research Institutions

Public Key Infrastructure

Hellenic Academic and Research Institutions Certification Authority (HARICA)

Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure

Version 4.11 (November 28th 2025)

Table of Contents

1 INTRODUCTION 12

1.1 OVERVIEW 12
1.2 DOCUMENT NAME AND IDENTIFICATION 13
1.3 PKI PARTICIPANTS 14
1.3.1 Certification Authorities 14
1.3.2 Registration Authorities 15
1.3.3 Subscribers 16
1.3.4 Relying Parties 16
1.3.5 Other participants 16
1.4 CERTIFICATE USAGE 17
1.4.1 Appropriate certificate uses 17
1.4.2 Forbidden certificate use 17
1.5 POLICY ADMINISTRATION 18
1.5.1 Policy Making Organization 18
1.5.2 Contact persons 18
1.5.3 Policy enforcement persons 19
1.5.4 CPS approval procedures 19
1.6 DEFINITIONS AND ACRONYMS 19
1.6.1 Definitions 19
1.6.2 Acronyms 34
1.6.3 References 35

2 PUBLICATION AND REPOSITORY 39

2.1 REPOSITORIES 39
2.2 DISCLOSURE OF CERTIFICATION AUTHORITY INFORMATION 39
2.3 FREQUENCY OF PUBLICATION 39
2.4 ACCESS CONTROLS ON REPOSITORIES 39

3 IDENTIFICATION AND AUTHENTICATION 40

3.1 NAMING 40
3.1.1 Type of Names 40
3.1.2 Obligation for meaningful names 40
3.1.3 Anonymity or pseudonymity of subscribers 40
3.1.4 Rules for interpreting various name forms 40
3.1.4.1 End-Entity Certificates for electronic signatures 41
3.1.4.2 End-Entity Certificates for electronic seals 42
3.1.4.3 End-Entity Certificates for SSL/TLS usage 42
3.1.4.4 End-Entity Certificates for Code Signing 43
3.1.4.5 End-Entity Certificates for Web Client Authentication 43
3.1.5 Uniqueness of names 44
3.1.6 Resolution Process regarding disputes about naming property rights and the role of trademarks 44
3.2 INITIAL IDENTITY VALIDATION 44
3.2.1 Method to prove possession of private key 45
3.2.2 Authentication of organization identity 45
3.2.2.1 Identity 46
3.2.2.2 DBA/Tradename/Roles 47
3.2.2.3 Verification of Country 47
3.2.2.4 Validation of Domain Authorization or Control 48
3.2.2.5 Authentication for an IP Address 58
3.2.2.6 Wildcard Domain Validation 61
3.2.2.7 Data Source Accuracy 61
3.2.2.8 CAA Records 62

3.2.2.9 Multi-Perspective Issuance Corroboration 64
3.2.3 Authentication of individual person identity 67
3.2.3.1 Entity applying for a user certificate 68
3.2.3.2 Individual who applies for a device certificate 70
3.2.4 Non verified subscriber information 71
3.2.5 Validation of Authority 71
3.2.6 Criteria for interoperability 71
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 72
3.3.1 Identification and authentication for routine re-key 72
3.3.2 Identification and authentication for re-key after revocation 72
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS 72
3.4.1 Revocation request from Issuing Authority 72
3.4.2 Revocation request from Subscriber 72
3.4.3 Revocation request from non-Subscriber 73

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 74

4.1 CERTIFICATE APPLICATION 74
4.1.1 Who is eligible to submit a certificate request 74
4.1.2 Enrollment process and responsibilities 74
4.1.2.1 Enrollment process for EV Certificates 74
4.2 CERTIFICATE APPLICATION PROCESSING 75
4.2.1 Subscriber identification and authentication procedures 75
4.2.2 Approval or rejection of certificate applications 76
4.2.3 Time to process certificate applications 77
4.2.4 Certificate Authority Authorization (CAA) 78
4.3 CERTIFICATE ISSUANCE 79
4.3.1 CA Actions during Certificate issuance 79
4.3.2 Notification to Subscribers by the CA regarding issuance of certificate 79
4.4 CERTIFICATE ACCEPTANCE 79
4.4.1 Conduct constituting certificate acceptance 79
4.4.2 Publication of the certificate by the CA 79
4.4.3 Notification of other entities about certificate issuance by the CA 79
4.5 KEY PAIR AND CERTIFICATE USAGE 80
4.5.1 Subscriber private key and certificate usage 80
4.5.2 Relying party public key and certificate usage 80
4.6 CERTIFICATE RENEWAL 80
4.6.1 Prerequisite Circumstances for certificate renewal 80
4.6.2 Who may request renewal 80
4.6.3 Processing certificate renewal requests 80
4.6.4 Notification of new certificate issuance to Subscriber 81
4.6.5 Conduct constituting acceptance of a renewal certificate 81
4.6.6 Publication of the renewal certificate by the CA 81
4.6.7 Notification of certificate issuance by the CA to other entities 81
4.7 CERTIFICATE RE-KEYING 81
4.7.1 Circumstance for certificate re-keying 81
4.7.2 Who may request certification of a new public key 81
4.7.3 Processing certificate re-keying requests 81
4.7.4 Notification of new re-keyed certificate issuance to Subscriber 81
4.7.5 Conduct constituting acceptance of a re-keyed certificate 81
4.7.6 Publication of the re-keyed certificate by the CA 81
4.7.7 Notification of re-keyed certificate issuance by the CA to other entities 81
4.8 CERTIFICATE MODIFICATION 82
4.8.1 Circumstance for certificate modification 82
4.8.2 Who may request certificate modification 82
4.8.3 Processing certificate modification requests 82
4.8.4 Notification of new certificate issuance to Subscriber 82

4.8.5 Conduct constituting acceptance of the certificate *82*
4.8.6 Publication of the modified certificate by the CA *82*
4.8.7 Notification of certificate issuance by the CA to other entities *82*
4.9 CERTIFICATE REVOCATION AND SUSPENSION 82
4.9.1 Circumstances for revocation *82*
4.9.1.1 Reasons for Revoking a Subscriber Certificate 82
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate 85
4.9.2 Who can request a revocation *86*
4.9.3 Procedure for revocation request *86*
4.9.3.1 Certificate revocation by the Subscriber 86
4.9.3.2 Certificate revocation by any other entity 86
4.9.3.3 Revocation request by an Application Software Supplier 86
4.9.3.4 Revocation request by the eIDAS National Supervisory Body 87
4.9.3.5 Revocation request by a National Competent Authority 87
4.9.4 Revocation request grace period *87*
4.9.4.1 Revocation dates for “Signature” Certificates 88
4.9.5 Time within which CA must process the revocation request *88*
4.9.6 Revocation checking requirement for relying parties *89*
4.9.7 CRL issuance frequency *89*
4.9.8 Maximum latency for CRLs *90*
4.9.9 Online revocation/status checking availability (OCSP) *90*
4.9.10 Online revocation checking requirements *91*
4.9.11 Other forms of revocation advertisements available *91*
4.9.12 Special requirements regarding key compromise *92*
4.9.12.1 Create and sign a test file 92
4.9.12.2 Create a CSR which includes a custom text 92
4.9.12.3 Disclose the actual Private Key 92
4.9.13 Circumstances for suspension *92*
4.9.14 Who can request suspension *93*
4.9.15 Procedure for suspension request *93*
4.9.16 Limits on suspension period *93*
4.10 CERTIFICATE STATUS SERVICES 93
4.10.1 Operational characteristics *93*
4.10.1.1 Online Certificate status service OCSP 93
4.10.1.2 Online Certificate Repository 94
4.10.1.3 Usage of Certificate Revocation Lists (CRL) 94
4.10.2 Service Availability *94*
4.10.3 Optional features *94*
4.11 END OF SUBSCRIPTION 94
4.12 KEY ESCROW AND RECOVERY 94
4.12.1 Key escrow and recovery policy and practices *94*
4.12.2 Session key encapsulation and recovery policy and practices *94*

5 ADMINISTRATIVE, TECHNICAL AND OPERATIONAL CONTROLS 95

5.1 PHYSICAL SECURITY AND ACCESS CONTROLS 95
5.1.1 Site location *95*
5.1.2 Physical access *95*
5.1.3 Power and cooling *95*
5.1.4 Water exposures *95*
5.1.5 Fire prevention and protection *95*
5.1.6 Media storage *95*
5.1.7 Waste Disposal *96*
5.1.8 Off-site backup *96*
5.2 PROCEDURAL CONTROLS 96
5.2.1 Trusted roles *96*
5.2.2 Number of persons required per task *96*
5.2.3 Identification and authentication for each role *96*

5.2.4 Roles requiring separation of duties ... 96
5.3 PERSONNEL CONTROLS ... 97
5.3.1 Qualifications, experience and clearance requirements ... 97
5.3.2 Background check procedures ... 97
5.3.3 Training requirements ... 97
5.3.4 Re-training frequency and requirements ... 97
5.3.5 Job rotation frequency and sequence ... 97
5.3.6 Sanctions for unauthorized actions ... 97
5.3.7 Independent contractor's requirements working outside GUnet and involved with the HARICA PKI ... 98
5.3.8 Documentation supplied to the personnel ... 98
5.4 AUDIT LOGGING PROCEDURES ... 98
5.4.1 Types of events recorded ... 98
5.4.1.1 Router and firewall activities logs ... 99
5.4.2 Frequency of processing audit log ... 100
5.4.3 Retention period for audit log ... 100
5.4.4 Protection of audit log ... 100
5.4.5 Audit log backup procedures ... 100
5.4.6 Audit collection system (internal vs. external) ... 100
5.4.7 Notification to event-causing subject ... 100
5.4.8 Vulnerability assessments ... 100
5.5 RECORDS ARCHIVAL ... 101
5.5.1 Types of records archived ... 101
5.5.2 Retention period for archive ... 101
5.5.3 Protection of archive ... 102
5.5.3.1 Access ... 102
5.5.3.2 Protection against the alteration of the records file ... 102
5.5.3.3 Protection against the deletion of the records file ... 102
5.5.3.4 Protection against the deterioration of storage media ... 102
5.5.3.5 Protection against future lack of availability of readers of the old media ... 102
5.5.4 Archive backup procedures ... 102
5.5.5 Requirements for time-stamping of records ... 102
5.5.6 Archive collection system (internal or external) ... 102
5.5.7 Procedures to obtain and verify archive information ... 102
5.6 KEY CHANGEOVER ... 103
5.7 COMPROMISE AND DISASTER RECOVERY ... 103
5.7.1 Incident and compromise handling procedures ... 103
5.7.1.1 Mass Revocation Plans ... 104
5.7.2 Computing resources, software and/or data are corrupted ... 104
5.7.3 Private key compromise procedures ... 105
5.7.4 Business continuity capabilities after a disaster ... 105
5.8 CERTIFICATION AUTHORITY OR REGISTRATION AUTHORITY TERMINATION ... 106

6 TECHNICAL SECURITY CONTROLS ... 107

6.1 KEY PAIR GENERATION AND INSTALLATION ... 107
6.1.1 Key pair generation ... 107
6.1.1.1 CA and TSU Key Pair Generation ... 107
6.1.1.2 RA Key Pair Generation ... 107
6.1.1.3 Subscriber Key Pair Generation ... 107
6.1.2 Private Key delivery to Subscriber ... 109
6.1.3 Public key delivery to certificate issuer ... 110
6.1.4 CA public key delivery to relying parties ... 110
6.1.5 Key sizes ... 110
6.1.6 Public key generation parameters and quality checking ... 111
6.1.7 Key usage purposes as per X.509v3 key usage field ... 112
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 112

6.2.1 Cryptographic module standards and controls ... *112*
6.2.2 Private Key control from multiple persons (N out of M) ... *112*
6.2.3 Private Key escrow ... *112*
6.2.4 Private Key backup ... *112*
6.2.5 Private Key archival ... *113*
6.2.6 Private Key transfer into or from a cryptographic module ... *113*
6.2.7 Private Key storage on cryptographic module ... *113*
6.2.7.1 Private key storage for CA keys ... 113
6.2.7.2 Private key storage for Timestamp Authorities ... 114
6.2.7.3 Private key storage for Signing Services ... 114
6.2.7.4 Subscriber Private Key protection and verification ... 114
6.2.8 Methods of activating private key ... *116*
6.2.8.1 Who can activate (use) a private key ... 116
6.2.8.2 Actions to be performed to activate a private key ... 116
6.2.8.3 Once activated, for how long is the key "active"? ... 116
6.2.9 Methods for deactivating private key ... *117*
6.2.10 Methods for destroying private key ... *117*
6.2.11 Cryptographic module rating ... *117*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT ... 117
6.3.1 Public key archival ... *117*
6.3.2 Certificate operational periods and key pair usage periods ... *117*
6.4 ACTIVATION DATA ... 118
6.4.1 Activation data generation and installation ... *118*
6.4.2 Activation data protection ... *118*
6.4.3 Other aspects of activation data ... *118*
6.5 COMPUTER SECURITY CONTROLS ... 119
6.5.1 Specific computer security technical requirements ... *119*
6.5.2 Computer security rating ... *119*
6.6 LIFE CYCLE TECHNICAL CONTROLS ... 119
6.6.1 System development controls ... *119*
6.6.2 Security management controls ... *119*
6.6.3 Life cycle security controls ... *119*
6.7 NETWORK SECURITY CONTROLS ... 119
6.8 TIME-STAMPING ... 120
6.8.1 Time-Stamp Issuance ... *120*
6.8.2 Time-Stamping Unit ... *120*
6.8.3 Time-Stamp Token ... *120*
6.8.4 Clock synchronization with UTC ... *121*

7 CERTIFICATE, CRL AND OCSP PROFILES ... 121

7.1 CERTIFICATE PROFILE ... 121
7.1.1 Version number ... *121*
7.1.2 Certificate Extensions ... *121*
7.1.2.1 Root CA Certificate ... 121
7.1.2.2 Intermediate CA Certificate ... 122
7.1.2.3 End-entity Certificate ... 124
7.1.2.4 All Certificates ... 128
7.1.3 Algorithm Object Identifiers ... *128*
7.1.3.1 SubjectPublicKeyInfo ... 128
7.1.3.2 Signature AlgorithmIdentifier ... 130
7.1.4 Name Forms ... *133*
7.1.4.1 Serial number ... 133
7.1.4.2 Signature Algorithm ... 133
7.1.4.3 Signature ... 133
7.1.4.4 Issuer ... 133
7.1.4.5 Valid From ... 134
7.1.4.6 Valid To ... 134
7.1.4.7 Subject Information ... 134

7.1.5 Name constraints *139*
7.1.6 Certificate policy object identifier *140*
7.1.7 Usage of Policy Constraints extension *143*
7.1.8 Policy qualifiers syntax and semantics *143*
7.1.9 Processing semantics for the critical Certificate Policies extension *143*
7.2 CRL PROFILE 143
7.2.1 Version number(s) *143*
7.2.2 CRL and CRL entry extensions *143*
7.2.2.1 Signature 143
7.2.2.2 Hashing Algorithm 144
7.2.2.3 Issuer Name 144
7.2.2.4 This Update 144
7.2.2.5 Next Update 144
7.2.2.6 Revoked Certificates 144
7.2.2.7 CRL Number (OID 2.5.29.20) 144
7.2.2.8 Authority Key Identifier 144
7.2.2.9 expiredCertsOnCRL (OID: 2.5.29.60) 144
7.2.2.10 reasonCode (OID 2.5.29.21) 144
7.2.2.11 issuingDistributionPoint (OID 2.5.29.28) 146
7.3 OCSP PROFILE 146
7.3.1 Version number *147*
7.3.2 OCSP extensions *147*

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 147

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 147
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 147
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 147
8.4 TOPICS COVERED BY ASSESSMENT 147
8.5 ACTIONS TAKEN BECAUSE OF DEFICIENCY 149
8.6 COMMUNICATION OF RESULTS 149
8.7 SELF-AUDITS 149

9 OTHER BUSINESS AND LEGAL MATTERS 150

9.1 FEES 150
9.1.1 Certificate issuance or renewal fees *150*
9.1.2 Certificate access fees *150*
9.1.3 Revocation or status information access fees *150*
9.1.4 Fees for other services *150*
9.1.5 Refund policy *151*
9.2 FINANCIAL RESPONSIBILITY 151
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 151
9.3.1 Scope of confidential information *151*
9.3.2 Information not within the scope of confidential information *151*
9.3.3 Responsibility to protect confidential information *151*
9.4 PRIVACY OF PERSONAL INFORMATION 151
9.4.1 Privacy plan *151*
9.4.2 Information treated as private *151*
9.4.3 Information not deemed private *152*
9.4.4 Responsibility to protect private information *152*
9.4.5 Notice and consent to use private information *152*
9.4.6 Disclosure pursuant to judicial or administrative process *152*
9.4.7 Other information disclosure circumstances *152*
9.4.7.1 Publicity 153
9.5 INTELLECTUAL PROPERTY RIGHTS 153
9.6 REPRESENTATIONS AND WARRANTIES 153
9.6.1 CA Representations and Warranties *153*
9.6.1.1 Responsibilities of externally-operated Certification Authorities 155

9.6.2 RA Representations and Warranties 155
9.6.3 Subscriber Representations and Warranties 156
9.6.4 Relying Party Representations and Warranties 158
9.6.5 Representations and Warranties of Other Participants 159
9.7 DISCLAIMERS OF WARRANTIES 159
9.8 LIMITATIONS OF LIABILITY 159
9.9 INDEMNIFICATION 160
9.10 TERM AND TERMINATION 161
9.10.1 Term and termination for Subscriber Agreements 161
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 161
9.12 AMENDMENTS 161
9.12.1 Procedure for amendment 161
9.12.2 Notification mechanism and period 162
9.12.3 Circumstances under which OID must be changed 162
9.13 DISPUTE RESOLUTION PROVISIONS 162
9.14 GOVERNING LAW 162
9.15 COMPLIANCE WITH APPLICABLE LAW 162
9.16 MISCELLANEOUS PROVISIONS 163
9.16.1 Entire Agreement 163
9.16.2 Assignment 163
9.16.3 Severability 163
9.16.4 Enforcement 164
9.16.5 Force Majeure 164
9.17 OTHER PROVISIONS 164
10 ANNEX A (HARICA ROOTS) 165
11 ANNEX B (HARICA COMMON CERTIFICATE PROFILES) 180
12 ANNEX C (HARICA HIERARCHY) 186
13 ANNEX D CAA CONTACT TAG 186
13.1 CAA METHODS 186
13.1.1 CAA contactemail Property 186
13.1.2 CAA contactphone Property 186
13.2 DNS TXT METHODS 187
13.2.1 DNS TXT Record Email Contact 187
13.2.2 DNS TXT Record Phone Contact 187
14 ANNEX E ISSUANCE OF CERTIFICATES FOR ONION DOMAIN NAMES 188
15 ANNEX F HARICA POLICY IDENTIFIERS 190

Version control

Version	Date	Comment
2.2	March 2011	• Adjusting to ETSI TS 101 456 "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates", additions • Definitions for certificate usage according to Greek legislation • Adjustments about Physical security and personnel security issues, CA private key restrictions (FIPS 140-2) • Private key protection • Decommission of MD5 hashing algorithm • Timestamping definitions • Certificate classes modifications for personal certificates • Modification on OCSP templates
2.3	May 2011	• Set minimum RSA key size 2048 bit • CRL, OCSP nextUpdate fields • Additions on how to verify personal Identification
2.4, 2.5	Nov-Dec 2011	• Adding NameConstraints
2.6	Apr 2012	• CodeSigning Certificates • Certificate store functionality
2.7	Apr 2013	• Incorporate CA/B Forum BR for Publicly-Trusted Certificates 1.1 • CRL, OCSP nextUpdate fields
3.0	Dec 2014	• Incorporate CA/B Forum BR for Publicly-Trusted Certificates 1.1.9 • Incorporate Microsoft Root Certificate Program –Technical Requirements 2.0

		• Incorporate Mozilla Root CA program Policy 2.2 • Adapt to Presidential Decree 150/2001 • Changes to certificate profiles and Policy OIDs
3.1	Feb 2015	• Adding qualified certificate extensions (qcStatements)
3.2	June 2015	• Changes at the allowed values of the Subject and the subjAltName extension • Disclosure of reviewing CAA records • Incorporate CA/B Forum BR 1.2.5
3.3	March 2016	• New Root CAs • Compliance to Updated Microsoft Root Program Policy • Incorporate CA/B Forum BR 1.3.1 • Improve compatibility with RFC 3647 • Improve compatibility with RFC 5480 (keyUsage bits for ECDSA certificates)
3.4	April 2016	• Refine language regarding the term “CA”, “TSP” • Added scope for cross-signing
3.5	May 2017	• Refine language regarding the term “Subordinate CA” • Changes to comply with ETSI EN 319 411-1. EN 319 411-2, EN 319 421 • Separate TimeStamping certificates from SSL, S/MIME, CodeSigning • Compliance with “Minimum Requirements of the Issuance and Management of Publicly-Trusted Code Signing Certificates” published at https://aka.ms/csbr (Effective date Feb 1st 2017)

		• Incorporate CA/B Forum BRs 1.4.5 • Change validity duration of end-entity SSL/Personal Certificates • New Insurance Contract for professional liability, updated liability rules
3.6	Feb 2018	• Incorporate CA/B Forum BRs 1.5.6 • Added language for Intellectual Property checks • Added language for key-pair generation for Code Signing Certificates and securing the Private Key
3.7	Oct 2018	• Minor typos • Support for Certificate Transparency • Allow Issued Certificates to be used for money transactions • Updated Certificate Problem Report reporting information • Provisions for suspending Certificates used for “Signing” • Clarifications for Certificate Re-key • Compliance to Mozilla Root Policy 2.6.1
3.8	Mar 2019	• Minor typos • Support for EV and QCP-w • Support for QCP-w-PSD2 • Allow for IP address values in SSL/TLS Certificates • Allow for Wildcard Certificates • Incorporate CA/B Forum BRs version 1.6.4 • Incorporate CA/B Forum EV Guidelines 1.6.8

		• Incorporate CA/B Forum EV Code Signing Guidelines 1.4 • Assign custom policy OIDs for each Certificate type
3.9	Oct 2019	• Update practices for EV Code Signing and remote QSCD • Update Annex with certificate profiles • Update definitions for Qualified Signatures/Seals • Change Name of GUnet • Update test URLs for User Agents
4.0	Mar 2020	• Add Registration Information about GUnet • Update Certificate Profiles • Adapt to Mozilla Root CA Program Policy 2.7 • Incorporation of BRs version 1.6.9 • Incorporation of EV Guidelines 1.7.1 • Update Revocation information • Removal of NONCE requirement for OCSP Responders • Reduce validity of SSL/TLS Certificates to 397 days starting 2020/08/01
4.1	Aug 2020	• Incorporation of BRs version 1.7.0 • Incorporation of EV Guidelines 1.7.2 • Clarify email validation methods using Domain Validation for the domain portion of email addresses • Add identity verification references to eIDAS • Update CRL signing frequency

		• Update section 6.1.1 for rejection of known weak and compromised keys • Update section 6.2.1 with references to remote QSCD and eIDAS art. 31 list. • Added policy OID for remote QSCD • Disclosure of Registration/Incorporation Agencies for EV Certificates
4.2	Sep 2020	• Clarify OCSP next update language • Explicitly prohibit MiTM use of Certificates • Incorporation of CA/B Forum Baseline Requirements for SSL/TLS Certificates 1.7.2 ballots SC28, SC35 • Incorporation of CA/B Forum EV Guidelines 1.7.3 • Incorporation of CA/B Forum Baseline Requirements for Code Signing Certificates 2.0 • Update Audit logging requirements • Update latest RFC for CAA • Update OCSP and CRL Profiles • Clarify disclosure practice of end-entity certificates on the Repository
4.3	Feb 2021	• Incorporation of CA/B Forum Baseline Requirements for SSL/TLS Certificates 1.7.3 • Remove the capability to issue TLS Certificates with no OCSP URI in the AIA extension, by enforcing OCSP stapling option for high-traffic Subscribers • Describe destruction of MBK as a method to destroy CA and TSU private key backups • Agreed-upon change to website is not allowed for Domain Namespace validation

		• Clarification about what Root Certificates can sign • Change Domain Name and IP address validation reuse period to 397 days • Stop using SSCD for issuance of Certificates for Qualified Signatures/Seals
4.4	May 2021	• Incorporation of CA/B Forum Baseline Requirements for SSL/TLS Certificates 1.7.4 • Incorporation of CA/B Forum EV Guidelines 1.7.3 • Incorporation of CA/B Forum Baseline Requirements for Code Signing Certificates 2.3 • Allow validation method for SSL/TLS wildcard onion Certificates • Effective 2021-06-01 forbid subject: organizationalUnitName field for SSL/TLS Certificates • Added HARICA Roots 2021 • Added explicit references to EV Guidelines for certain criteria • Remove exception for CAA checks when an Affiliate of HARICA is the DNS Administrator of a Domain • Support for all eIDAS identity proofing methods • Typographical errors corrected
4.5	Mar 2022	• Revoke within 24 hours certificates associated with “weak keys” demonstrated or proven that it is possible to calculate the Private Key based on the Public Key • Incorporation of CA/B Forum Baseline Requirements for SSL/TLS Certificates 1.8.2

		• Incorporation of CA/B Forum EV Guidelines 1.7.8
		• Incorporation of CA/B Forum Baseline Requirements for Code Signing Certificates 2.7
		• Incorporation of
		  ○ ETSI EN 319 401 v2.3.1
		  ○ ETSI EN 319 411-1 v1.3.1
		  ○ ETSI EN 319 411-2 v2.4.1
		  ○ ETSI EN 319 412-1 v1.4.4
		• Change identity validation reuse period for Qualified Certificates for eSignatures/eSeals
		• Incorporation of Ministerial Decision 27499/2021-08 for Remote Identity Proofing
		• Support for separation of QCP-w into QEVCP-w and QNCP-w of ETSI EN 319 411-2 v2.4.1
		• Support for LEI
		• Update key pair usage periods
		• Support for short-term certificates
		• Improve language for Certificate Profiles

4.6	Oct 2022	• Incorporation of CA/B Forum Baseline Requirements for SSL/TLS Certificates 1.8.4 • Incorporation of CA/B Forum EV Guidelines 1.7.9 • Incorporation of CA/B Forum Baseline Requirements for Code Signing Certificates 3.0.0+CSC-17 • Specify revocation reasons under certain circumstances

		• Removal of reference to EV Code Signing Requirements as obsolete • Allow subscriber key-pairs generated in software to be reused for 5 years • Reduce validity of code signing and S/MIME Certificates to 824 days • Prefer SHALL instead of MUST for consistency
4.7	July 2023	• Incorporation of CCADB Policy 1.2.1 • Incorporation of Chrome Root Program Policy 1.4 • Incorporation of CA/B Forum Baseline Requirements for SSL/TLS Certificates 1.8.7 • Incorporation of CA/B Forum EV Guidelines 1.8.0 • Incorporation of CA/B Forum Baseline Requirements for Code Signing Certificates 3.2.0 • Incorporation of CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificate 1.0.0 • Update subscriber key pair generation methods for “Class A” Certificates • Clarified language to better match the expectations of CA/B Forum policies/practices
4.8	July 2024	• Set maximum validity from 397 to 398 days • Updates based on Regulation (EU) 1183/2024 • Incorporation of CCADB Policy 1.3.0 • Incorporation of Chrome Root Program Policy 1.5

		• Incorporation of Mozilla Root Store Policy 2.9 • Incorporation of CA/B Forum Baseline Requirements for SSL/TLS Certificates 2.0.5 • Incorporation of CA/B Forum Baseline Requirements for Code Signing Certificates 3.7.0 • Incorporation of CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificate 1.0.4 • Incorporation of CA/B Forum EV Guidelines 2.0.1 • Add support for id-kp-docSigning KeyPurposeId • Clarification about Key Generation by HARICA in Subscriber Warranties • Fix typos

4.9	March 2025	• Update Organizationidentifier under Subject Information according to the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
		• Incorporation of Microsoft Trusted Root Program Requirements (2024-02-15)
		• Incorporation of Chrome Root Program Policy 1.6
		• Incorporation of Mozilla Root Store Policy 3.0
		• Incorporation of CCADB Policy 1.3.1
		• Incorporation of
		  o ETSI EN 319 401 v3.1.1
		  o ETSI EN 319 411-1 v1.4.1

		○ ETSI EN 319 411-2 v2.5.1 ○ ETSI EN 319 412-1 v1.5.1 ○ ETSI EN 319 412-2 v2.3.1 ○ ETSI EN 319 412-3 v1.3.1 ○ ETSI EN 319 412-4 v1.3.2 ○ ETSI EN 319 421 v1.2.1 ○ ETSI TS 119 411-6 v1.1.1 ○ ETSI TS 119 495 v1.7.1 • Incorporation of CA/B Forum: ○ Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 2.1.4 ○ Baseline Requirements for Code Signing Certificates 3.9 ○ Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates 1.0.8 • Added support for QNCP-w-gen • Removal of HARICA ROOT CA 2011
4.10	June 2025	• Fix typos • Updated Certificate acceptance process • Update Certificate Problem Report reporting mechanisms and process • Incorporation of CA/B Forum: ○ Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 2.1.5 ○ Baseline Requirements for the Issuance and Management of

		Publicly-Trusted S/MIME Certificates 1.0.8
4.10.1	June 2025	• Added availability for Time-stamping Authority

4.11	November 2025	• Incorporation of CA/B Forum:
		  ○ Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 2.1.9 + Ballots SC86, SC90, SC91
		  ○ Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates 1.0.12
		  ○ Baseline Requirements for Code Signing Certificates 3.1
		  ○ Network and Certificate System Security Requirements 2.0.5
		• Incorporation of Chrome Root Program Policy 1.7
		• Incorporation of Microsoft Trusted Root Program Requirements 1.0
		• Incorporation of CCADB Policy 2.0
		• Enforce DNSSEC validation for CAA and non-email DCV methods
		• Mass-certificate-revocation plan
		• Added support for Domain Validation method “DNS Labeled with Account ID – ACME”

1 Introduction

The Public Key Infrastructure (PKI) for the Hellenic Academic and Research Institutions is supported and operated by the **Greek Universities Network (GUnet)** (https://www.gunet.gr), a non-profit civil law company with members all the Universities of Greece, with VAT number **EL099028220**, General Commercial Registry number **160729401000** and Registration of Incorporation number **13392/28-9-2000** lawfully registered in the company's records of the Athens Court of First instance. This GUnet service, hereafter referred to as the Hellenic Academic and Research Institutions Certification Authority (HARICA), acts as a Trust Service Provider (TSP) also known as a "Certification Authority", and as a "Qualified" Trust Service Provider (QTSP). For the rest of this CP/CPS, the terms "TSP" and "QTSP" will be used equally.

HARICA specifically acts as a "Root CA Operator". The development and initial operation of the service began as part of the Virtual Network Operations Center (VNOC) project, funded by the National Research Network – GRNET (https://www.grnet.gr) and continues under the supervision and funding of GUnet. HARICA is operated and managed by Aristotle University of Thessaloniki's IT Center, one of the members of GUnet. Organizations involved in this Public Key Infrastructure unconditionally accept this Certificate Practice Statement / Certificate Policy and co-sign a Memorandum of Understanding.

1.1 Overview

This Certificate Policy and Certification Practice Statement, describes the set of rules and procedures concerning digital certificates within the HARICA Public Key Infrastructure.

HARICA, acting as a "Root CA Operator" issues Subordinate CA Certificates and end-entity Certificates for Natural and Legal Entities. HARICA also issues Time-Stamps and Qualified Time-Stamps. All end-entity Certificates contain a reference to this document or a CP/CPS of a Subordinate CA Operator. Certificate owners and relying parties, must be aware of this policy document and must comply with its statements.

HARICA for its Public Key Infrastructure complies with:

- ETSI EN 319 401 v3.1.1. "General Policy Requirements for Trust Service Providers",
- ETSI EN 319 411-1 v1.4.1. "Policy and security requirements for Trust Service Providers issuing certificates; Part1: General requirements" under the scope NCP, NCP+, LCP, DVCP, OVCP, EVCP,
- ETSI EN 319 411-2 v2.5.1. "Policy and security requirements for Trust Service Providers issuing certificates; Part2: Requirements for Trust Service Providers issuing EU qualified certificates" under the scope QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QNCP-w, QNCP-w-gen, QEVCP-w,
- ETSI EN 319 421 v1.2.1. "Policy and security requirements for Trust Service Providers issuing Time-Stamps" under the scope BTSP,
- Qualified Trust Service Provider (QTSP), following eIDAS.

In addition to the above standards, HARICA complies with

- ETSI TS 119 411-6 v1.1.1 "Policy and security requirements for Trust Service Providers issuing certificates; Part6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates",
- ETSI TS 119 495 v1.7.1 that supports Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366, the Delegated Regulation (EU) 2018/389 with regard to Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication under the scope QCP-w and QCP-w-psd2, and
- the Ministerial Decision 27499/2021-08 for Remote Identity Proofing.

Finally, if a HARICA self-signed root CA certificate is included in an Application Software Supplier's Root Store after HARICA's application for inclusion in that Root Store, HARICA SHALL comply with policies defined by that Application Software Supplier and shall ensure continued compliance of all corresponding subordinate CAs and Delegated Third Parties participating in HARICA's PKI.

1.2 Document Name and identification

This document is called «Certificate Policy and Certification Practice Statement of HARICA Public Key Infrastructure» and constitutes the documentation and regulatory framework of HARICA Public Key Infrastructure. In abbreviation, it will be referred to as "HARICA CP-CPS".

The Certificate Policy's purpose is to determine, document and make known to all interested entities (e.g. members of the academic community, collaborators, third-party entities that rely on the provided services, other organizations, Institutions and Authorities, Subscribers) the terms and the operational practices that are applied or govern the Certification Services that HARICA provides.

The structure of this document is based on the outline set forth in section 6 of IETF RFC 3647, as amended by the CA/Browser Forum Baseline Requirement documents. HARICA conforms to the current version of the

- "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates",
- "Guidelines for the Issuance and Management of Extended Validation Certificates",
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Code Signing Certificates",
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates",

published at https://www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document. This means that HARICA shall continuously keep track of changes in CA/B Forum documents and incorporate the changes before their effective dates and update this CP/CPS accordingly.

The globally unique Identification Number (OID) of this document is: 1.3.6.1.4.1.**26513.1.0.4.11** where:

1.3.6.1.4.1.**26513**	Identification Number (OID) of HARICA, registered to IANA (www.iana.org)
1	Certification Services Provision
0	Certification Practice Statement
4.11	First and Second digit of the version number of the Certification Practice Statement (plus possible minor revision number)

1.3 PKI Participants

The entities including Natural Persons (collectively referred to hereon as "entities") that use digital certificates issued by HARICA, constitute the community governed by this Certificate Policy and Certification Practice Statement.

1.3.1 Certification Authorities

Certification Authorities (CAs) are the entities of the Public Key Infrastructure responsible for issuing and managing digital Certificates. These Certificates flow down from Root CA Certificates (usually publicly trusted) and successive Subordinate CA Certificates.

The hierarchy of HARICA acting as a Trust Service Provider is constituted by the following entities:

1. **Root CAs**, which issue Subordinate CA Certificates exclusively and do not issue certificates for end-entities. As an exception, it is allowed to issue certificates for OCSP responders according to section 4.2.2.2 of RFC 6960. Subordinate CA Certificates are either issued for Externally Operated Subordinate CAs or Internally Operated Subordinate CAs.
2. **Internally Operated Subordinate CAs**, which are under the control of HARICA as a Root CA Operator, on behalf of organizations affiliated with HARICA that comply with and fully adopt this Certificate Policy and Certification Practice Statement. The validity period of the Subordinate CA Certificates is eight (8) to fifteen (15) years. In the case where an Internally Operated Subordinate CA follows different policy and certification practices compared to this document, a separate CP/CPS document must be created (with a unique OID). Internally Operated Subordinate CAs may include Issuing CAs for limited scope (e.g. Time-Stamping, Code Signing, SSL/TLS, Client-S/MIME) under the control of HARICA as a Root CA Operator.
3. **Externally Operated Subordinate CAs**, which must be properly audited or technically constrained according to section 7.1.5 and according to policies set forth by the Root programs of Apple, Google, Microsoft, Mozilla and comply with eIDAS. In the case of Externally Operated Subordinate CAs, an OID with the Subordinate CA's CP/CPS SHALL BE included in the appropriate policy extension field of the corresponding Subordinate CA Certificate.
4. HARICA may issue cross-certificates per section 3.2.6.

The CA hierarchy, as of the date this CP/CPS is published, is available in ANNEX C (HARICA Hierarchy).

1.3.2 Registration Authorities

Registration Authorities (RA) are entities responsible for identity validation of all Applicants before the issuance of the certificate. They transfer the requests to a particular Issuing CA in a secure manner. HARICA operates a Central Registration Authority to verify Applicant identities, domain control and all related vetting and validation procedures prior to the issuance of a Certificate.

HARICA may utilize registration offices of Affiliates for identification of Applicants that request certificates that belong to the corresponding Affiliate organization. This method resembles the "Enterprise RA" model to verify certificate requests from the "Enterprise RA's" own organization. These certificates must be scoped to the Affiliate Organization's Domain Namespace.

HARICA SHALL NOT delegate validation of the domain portion of an email address and the performance of validation actions of sections 3.2.2.4, 3.2.2.5 and 3.2.2.8 to a Delegated Third Party.

The Central Registration Authority also validates entities associated with internal HARICA operations (HARICA operators and Certificates for infrastructure purposes).

Before HARICA authorizes a Delegated Third Party to perform a delegated function, HARICA SHALL contractually require the Delegated Third Party to:

1. Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
2. Retain documentation in accordance with Section 5.5.2;
3. Abide by the other provisions of this CP/CPS that are applicable to the delegated function; and
4. Comply with this CP/CPS or the Delegated Third Party's practice statement that HARICA has verified complies with this CP/CPS.

HARICA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

HARICA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. HARICA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace.
2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, HARICA SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject.

HARICA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

1.3.3 Subscribers

PKI Subscribers are defined in section 1.6.1 and are entities who request and successfully acquire a digital certificate issued by a Subordinate CA that chains to one of HARICA's publicly trusted Root CA Certificates. In the case of Time-Stamps, Subscribers are entities that have agreed to this CP/CPS and acquired a TST from a HARICA TSU.

The subscription of roles (e.g. 'Rector', 'president') or persons that are not real, apart from network devices or services, is neither explicitly foreseen in the current document nor forbidden. The issuance of 'role certificates' is possible by a Subordinate CA, provided that the relevant procedure is described in a separate CPS or included in a future revision of this CP/CPS and that this procedure does not conflict with any condition of the current document.

1.3.4 Relying Parties

The entities that trust the provided certification services or otherwise called the Relying Parties can be any entity, which uses in any way the certification tokens (digital certificates, digital signatures, time stamps etc.) and relies on the information that they contain.

In particular, entities that trust the Certification Services are the natural persons or legal entities who, after being informed and having agreed with the terms and conditions concerning the use of the certificates as described in the present document and the relative certificate policy, and after having checked and verified the validity of a certificate that has been issued by HARICA, they decide whether they can rely on the content of this certificate in order to proceed to specific actions or justified belief.

In order to verify the validity of the signature created by a Certificate, Relying Parties must check that:

- √ The certificate was within its validity period.
- √ The certificate is correctly chained to a HARICA Subordinate CA Certificate that chains to one of HARICA's publicly trusted Root CA Certificates.
- √ The certificate was not revoked for any reason when the signing operation occurred.
- √ Subject identification matches the details that the signer presents.
- √ The usage of the certificate matches the intended usage it was issued for, by HARICA.
- √ The terms and conditions as described in the present CP/CPS are fulfilled.

1.3.5 Other participants

HARICA Subscribers may choose to use a third-party remote QSCD provider. Such a remote QSCD provider must be a QTSP, properly audited under the eIDAS regulation by a Qualified Auditor and in conformity with the requirements of section 8 of the current CP/CPS and Article 20 of eIDAS. HARICA shall verify that this third-party TSP is meeting appropriate requirements in terms of qualification.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

HARICA Certificates can be used for authentication, encryption, access control and digital signing, in all network services and applications in which the required level of security is equal or lower than that of the certificate issuance process.

Typical applications in which digital certificates issued by HARICA can be used, are the following (the list is not restrictive):

a) Signing of an "electronic document" by a natural person or legal entity using a digital certificate and the relevant private key, preferably with the use of a "Secure Signature Creation Device" SSCD or a "Qualified Signature/Seal Creation Device" QSCD (e.g. smart card or e-token), so that at least the following characteristics are ensured:

1) the authenticity of origin,

2) the integrity of the signed document i.e. that its content has not been modified since the time of its' signature and

3) the binding of the signatory to the content of document and the non-repudiation of signature.

b) Signing of email messages, as a proof of authenticity of the sender's email address and for all the attributes described in (a). Moreover, they can be used for secure proof of receipt of messages (non-repudiation of receipt).

c) Persistent proof of identity (Strong Authentication) of a user or a device throughout communication with other entities, guaranteeing high-level security characteristics, stronger than the ones provided by password-based access control methods.

d) "Encryption of documents and messages" with the use of the recipient's publicly available certificate, ensuring that only she/he, the holder of corresponding private key, can decipher and read the document or the message.

e) Certification of other Trust Service Providers or other additional services of certification, e.g. time-stamping, digital notarization and long-term secure preservation of data.

f) In the implementation of secure network protocols, such as SSL/TLS, IPSec etc.

HARICA also operates as a Qualified Time-Stamping Authority providing Qualified and non-Qualified Time-Stamp Tokens. If a TSU issues time-stamps that are claimed to be qualified electronic time-stamps as per eIDAS, this TSU shall not issue non-qualified electronic time-stamps.

1.4.2 Forbidden certificate use

Certificates cannot be used for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger of life or any other uses that are not included in the first paragraph of section 1.4.1.

TLS Server Certificates shall not be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the certificate holder does not legitimately own or control. Such certificate usage is explicitly prohibited.

1.5 Policy administration

1.5.1 Policy Making Organization

This CP/CPS and all subscriber/third-party agreements, security policy documents and procedural documents, are administered by HARICA Policy Management Committee (PMC), appointed by the GUnet governing board.

ca-admin at harica.gr
Greek Universities Network GUnet
National and Kapodestrian University of Athens – Network Operations Center
University Campus 157 84
Tel: +30-210 7275611
Fax: +30-210 7275601

1.5.2 Contact persons

ca at harica.gr
Dimitris Zacharopoulos [dzacharo at harica.gr]
Tel: 2310 998483
Fax: 2310 999100

Ioannis Salmatzidis [jsal at it.auth.gr]
Tel: 2310 998498
Fax: 2310 999100

Spiros Bolis [sbol at gunet.gr]
Tel: 210 7275611
Fax: 210 7275601

Hellenic Academic and Research Institutions Certification Authority
Greek Universities Network GUnet
National and Kapodestrian University of Athens – Network Operations Center
University Campus 157 84
Tel: +30-2310 998483, +30-2310 998435
Fax: +30-2310 999100

Contact HARICA for Certificate Problem Reports by sending an email to "**cert-problem-report at harica.gr**".

HARICA also maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report to the email address **"high-priority-cert-problem-report at harica.gr"**, and where appropriate, forward such a complaint to competent public authorities, and/or revoke a Certificate that is the subject of such a complaint.

HARICA has also implemented web forms (https://www.harica.gr/en/Contact/CPR) that can be used to submit Certificate Problem Reports using a Browser.

In the unlikely event that the email addresses "**cert-problem-report at harica.gr**" does not work properly and the reported email is returned as undelivered, the reporting party

shall use the **"high-priority-cert-problem-report at harica.gr"** email address as a backup.

Also see sections 4.9.3.2 and 4.9.3.3.

1.5.3 Policy enforcement persons

cp at harica.gr
Dimitris Zacharopoulos [dzacharo at harica.gr]
Tel: +30-2310 998483

Ioannis Salmatzidis [jsal at it.auth.gr]
Tel: +30-2310 998498

Spiros Bolis [sbol at gunet.gr]
Tel: +30-210 7275611

Certification Authority Management
Greek Universities Network GUnet
National and Kapodestrian University of Athens – Network Operations Center
University Campus 157 84
Tel: +30-2310 998483, +30-2310 995000

1.5.4 CPS approval procedures

The CP/CPS is approved by the Policy Management Committee. All amendments and updates shall be posted at a publicly accessible Repository. HARICA SHALL disclose new versions of this CP/CPS to the CCADB before the corresponding changes are put into practice.

Major changes to the CP/CPS shall be contacted to Subscribers with due notice, in any convenient way, before they become effective.

HARICA regularly monitors industry Forums such as Mozilla dev-security-policy and "ca-compliance" incidents disclosed in https://bugzilla.mozilla.org. HARICA also participates as a voting Member in the CA/Browser Forum (https://cabforum.org) and ETSI ESI Technical Committee (https://www.etsi.org/committee/esi).

Even if there is no compulsory reason for a change in this CP/CPS, the PMC performs a review process at least annually to improve policies and practices (opportunity for improvement) and updates this CP/CPS accordingly.

1.6 Definitions and acronyms

The Definitions found in the CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

1.6.1 Definitions

Advanced Electronic Seal: An electronic signature that meets the requirements of Article 36 of eIDAS.

Advanced Electronic Signature: An electronic signature that meets the requirements of Article 26 of eIDAS.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, 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 acting on behalf of the Applicant, in a legally binding manner, who is employed either by the Applicant or an agent duly authorized to represent the Applicant:

(i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or
(ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or
(iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of HARICA.

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

Attestation Letter: A letter attesting that Subject Information is correct written by a 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. The coverage rules and maximum length of audit periods are described 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 audited standards listed in section 8.4.

Authorization Domain Name: The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. HARICA 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 HARICA SHALL remove "`*.`" from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. HARICA 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 Port: 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.

CA Certificate: A Certificate in which the `basicConstraints` extension has the `cA` attribute set to TRUE.

Certification Authority Authorization:

- For server TLS Certificates, CAA is defined in RFC 8659: "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".
- For S/MIME Certificates, CAA is defined in RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain."

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 Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

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

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

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

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 Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7.

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

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

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.

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

Certificate Transparency: An “append-only” public logging Certificate system as described by RFC 6962.

Code Signing Certificate: A digital certificate that contains a code Signing EKU and is trusted in an Application Software Provider’s root store to sign software objects

Common CA Database: Also known as the “CCADB”. This is a repository of information about externally operated Certification Authorities (CAs) whose root and intermediate certificates are included within the products and services of CCADB Root Store Operators (https://ccadb.org)

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%.

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6

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

Cross Certificate: A certificate that is used to establish a trust relationship between two Root 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 HARICA but is authorized by HARICA to assist in the Certificate Management Process by performing or fulfilling one or more of HARICA's requirements found herein.

DNS CAA Email Contract: The email address defined in section 13.1.1.

DNS CAA Phone Contract: The email address defined in section 13.1.2.

DNS TXT Record Email Contact: The email address defined in section 13.2.1.

DNS TXT Record Phone Contact: The phone number defined in section 13.2.2.

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 that 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 Registrar: 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).

EBA PSD2 Register: register of payment institutions and e-money institutions developed, operated and maintained by the EBA under article 15 of Directive (EU) 2015/2366.

eIDAS Regulation: Refers to Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024.

Enterprise EV Certificate: An EV Certificate that an Enterprise RA authorizes HARICA to issue at third and higher domain levels. Enterprise EV SSL/TLS Certificates can only be issued at third and higher domain levels.

Enterprise EV RA: An employee or agent of an organization unaffiliated with HARICA who authorizes HARICA to issue EV Certificates.

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

European Unique Identifier (EUID): The EUID uniquely identifies officially-registered organizations, Legal Entities, and branch offices within the European Union or the European Economic Area. The EUID is specified in chapter 9 of the Annex contained in the Implementing Regulation (EU) 2021/1042 which describes rules for the application of Directive (EU) 2017/1132 "relating to certain aspects of company law (codification)".

EV Certificate: A certificate that contains subject information specified in, and which has been validated in accordance with the EV Guidelines. There are EV Certificates for SSL/TLS and for Code Signing. Both certificate types follow the same practices for validation Subject Information related to the Identity of the Applicant.

EV Certificate Renewal: The process whereby an Applicant who has a valid, unexpired and non-revoked EV Certificate issued by HARICA, makes an application for a newly issued EV Certificate that includes the same organizational name and Domain Name as the existing EV Certificate, a new “valid to” date beyond the expiry of the current EV Certificate and the application is prior to the expiration of the Applicant’s existing EV Certificate.

EV Certificate Request: A request from an Applicant requesting an EV Certificate whose valid request is authorized by the Applicant and signed by the Applicant Representative.

EV Code Signing Guidelines: The document “Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates”, published and maintained by the CA/B Forum.

EV Guidelines: The document “Guidelines For The Issuance And Management Of Extended Validation Certificates”, published by the CA/B Forum. This document mainly focuses on SSL/TLS Certificates but some of these requirements are referenced by EV Code Signing Guidelines and ETSI European Norms (e.g. ETSI EN 319 411-1).

EV Processes: The keys, software, processes, and procedures by which HARICA verifies Certificate Data, issues EV Certificates, maintains a Repository and revokes EV Certificates.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Externally Operated Subordinate CA: A third party Subordinate CA Operator, not affiliated with HARICA, that is in possession or control of a Private Key associated with a Subordinate CA Certificate issued by HARICA.

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, county, etc.).

Hardware Crypto Module: A tamper-resistant device, with a cryptography processor, used for the specific purpose of protecting the lifecycle of cryptographic keys (generating, managing, processing, and storing).

High Risk Certificate Request: A Request that HARICA flags for additional scrutiny by reference to internal criteria and databases maintained by HARICA, 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 HARICA identifies using its own risk-mitigation criteria.

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Internally Operated Subordinate CA: A Subordinate CA, operated by HARICA or its Affiliate that is in possession or control of the Private Key associated with the Subordinate CA Certificate.

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).

IP Reverse Zone Suffix: One of the two FQDNs that consist of the Domain Labels "in-addr.arpa" or "ip6.arpa". These two FQDNs serve as the root of the IP version 4 and IP version 6 reverse mapping space. "in-addr.arpa" is the root of the IP version 4 reverse mapping space and "ip6.arpa" is the root of the IP version 6 reverse mapping space.

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.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.

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.

Latin Notary: A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.

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, as the subject of rights and obligations in a country's legal system.

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal Practitioner: A person who is either a lawyer or a Latin Notary (see above) and competent to render an opinion on factual claims of the Applicant.

Lifetime Signing OID: An optional extended key usage OID (1.3.6.1.4.1.311.10.3.13) used by Microsoft Authenticode to limit the lifetime of the code signature to the expiration of the code signing certificate.

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."

Notary: A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document

Non-EV Code Signing Certificate: Term used to signify requirements that are applicable to Code Signing Certificates which do not have to meet the EV Code Signing requirements.

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 and providing Online Certificate Status Protocol responses. See also, Online Certificate Status Protocol.

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.

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.

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.

Parent Company: A company that Controls a Subsidiary Company.

Persistent DCV TXT Record: A DNS TXT record identifying an Applicant in accordance with Section 3.2.2.4.22.

Penetration Test: A process that identifies and attempts to exploit openings and vulnerabilities on the Certificate System through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

Platform: The computing environment in which an Application Software Supplier uses Certificates and incorporates Root Certificates as Trust Anchors.

Precertificate: As described in RFC 6962, it is constructed from the certificate to be issued by adding a special critical "poison extension" (OID 1.3.6.1.4.1.11129.2.4.3), whose extnValue OCTET STRING contains ASN.1 NULL data (0x05 0x00)) to the end-entity TBSCertificate. This extension is to ensure that the Precertificate cannot be validated by a standard X.509v3 client.

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 Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

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.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of section 8.2 (Auditor Qualifications).

Qualified Certificate for electronic seal: A Certificate for Qualified Electronic Seal that is issued by a qualified trust service provider and meets the requirements of Annex III of eIDAS.

Qualified Certificate for electronic signature: A Certificate for Qualified Electronic Signatures that is issued by a qualified trust service provider and meets the requirements of Annex I of eIDAS.

Qualified Electronic Seal: An Advanced Electronic Seal that is created by a Qualified Electronic Seal Creation Device, and which is based on a Qualified Certificate for Electronic Seal, as eIDAS.

Qualified Electronic Signature: An Advanced Electronic Signature that is created by a Qualified Electronic Signature Creation Device, and which is based on a Qualified Certificate for electronic signatures, as specified in eIDAS.

Qualified Electronic Signature/Seal Creation Device: Also known as QSCD. An electronic signature creation device that meets the requirements of Annex II of eIDAS.

Qualified Electronic Time-stamp: An electronic Time-stamp that meets the requirements of Article 42 of eIDAS.

Registration Agency: A Governmental Agency that registers business information in connection with an entity’s business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency may include, but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a

federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registration Authority: 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.

Registration Number: The unique number assigned to a Private Organization by the Incorporating Agency in such entity’s Jurisdiction of Incorporation.

Random Value: A value specified by HARICA 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 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.

Registration Reference: An identifier assigned to a Legal Entity.

Registration Scheme: A scheme for assigning a Registration Reference meeting the requirements identified in Clause 5.1.4 of ETSI EN 319 412-1.

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.

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 HARICA 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 HARICA 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.

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

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

Reverse Zone Domain Name: the FQDN in the `.arpa` namespace that corresponds to an IP address. This FQDN is constructed by converting the IP address to a sequence of labels followed by the applicable IP Reverse Zone Suffix, as specified in RFC 1035 (for IPv4 addresses) and RFC 3596 (for IPv6 addresses).

Root CA Operator: The top-level Certification Authority (i.e. an organization) whose CA Certificate (or associated Public Key) is distributed by Application Software Suppliers as a trust anchor.

Root CA Certificate: A CA Certificate in which the Public Key has been digitally signed by its corresponding Private Key.

Short-lived Subscriber Certificate: See Short-term Certificate.

Short-term Certificate: Certificate whose Validity Period is shorter than the maximum time to process a revocation request. For server TLS Certificates issued on or after 15 March 2024 and prior to 15 March 2026, the Validity Period is less than or equal to 10 days (864,000 seconds). For server TLS Certificates issued on or after 15 March 2026, the Validity Period is less than or equal to 7 days (604,800 seconds).

Signing Service: An organization that generates the Key Pair and securely manages the Private Key associated with a Signing Certificate, on behalf of a Subscriber.

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

Superior Government Entity: Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of the Applicant.

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 or an IP Address listed in the `subjectAltName` extension or the Subject `commonName` field.

Subordinate CA: A Certification Authority in possession or control of the Private Key associated with a Subordinate CA Certificate. A Subordinate CA Operator is either an Externally Operated Subordinate CA or an Internally Operated Subordinate CA.

Subordinate CA Certificate: A CA Certificate that has been signed by the Private Key associated with a Root CA Certificate or a different Subordinate CA Certificate

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

Subscriber Agreement: An agreement between HARICA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

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

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, code that compromises user security and/or code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes.

Takeover Attack: An attack where a Private Key associated with a Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate that uses a combination of Extended Key Usage settings and Name Constraint settings 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 this CP/CPS when the Applicant/Subscriber is an Affiliate of HARICA or IS HARICA.

Time-Stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

Time-Stamp Token (TST): a data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.

Time-Stamping Authority (TSA): TSP providing time-stamping services using one or more time-stamping units.

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

Top-Level Domain: From RFC 8499 (https://tools.ietf.org/html/rfc8499): “A Top-Level Domain is a zone that is one layer below the root, such as ”com” or “jp”.”

TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory 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.

UTC(k): time scale realized by the certified laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

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

Validation Specialist: A person who performs the information verification duties specified by this CP/CPS.

Validity Period (of a Certificate): The period-of-time from `notBefore` through `notAfter`, inclusive.

Vulnerability Scan: A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities.

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 9082, or an HTTPS website.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names 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 (https://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

Short Term	Explained Term
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CCADB	Common CA Database
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As
DN	Distinguished Name
DVCP	Domain Validation Certificates Policy
EBA[1]	European Banking Authority
EIDAS	eIDAS Regulation
EKU	Extended Key Usage
EV	Extended Validation
EVCP	Extended Validation Certificates Policy
FIPS	United States Federal Information Processing Standards
FQDN	Fully-Qualified Domain Name
QIIS	Qualified Information Source
QSCD QSealC	Qualified Signature/Seal Creation Device Qualified electronic Seal Certificate
QTSP QWAC	Qualified Trust Service Provider Qualified Website Authentication Certificate
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T NCA[1]	ITU Telecommunication Standardization Sector National Competent Authority
OCSP	On-line Certificate Status Protocol

[1] See Directive (EU) 2015/2366

OID	International Standards Organization's Object Identifier
OVCP	Organizational Validation Certificates Policy
PIN	Personal identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	IETF Working Group on PKI
PMC	Policy Management Committee
PSD2[1]	Payment Services Directive 2
PSP[2]	Payment Service Provider
PSP_AI[2]	Account Information Service Provider
PSP_AS[2]	Account Servicing Payment Service Provider
PSP_IC[2]	Payment Service Provider Issuing Card-based payment instruments
PSP_PI[2]	Payment Initiation Service Provider
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSCD	Secure Signature Creation Device
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Socket Layer
subCA	Subordinate Certification Authority
TLD	Top Level Domain
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
X.509	ITU-T standard for Certificates and authentication framework

1.6.3 References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part2: Requirements for Trust Service Providers issuing EU qualified certificates

[2] See Commission Delegated Regulation (EU) 2018/389

ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Time-Stamps

ETSI TS 119 495, Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

FIPS 140-3, Federal Information Processing Standards Publication – Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019.

FIPS 186-5, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, February 2023.

ISO 21188:2018, Public key infrastructure for financial services – Practices and policy framework.

Network and Certificate System Security Requirements, Version 2.0.5, available at https://cabforum.org/2025/06/03/ballot-ns-008/CA-Browser-Forum-FG-NCSSR-2.0.5.pdf.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, https://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997.

RFC3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. S. Chokhani, et al. November 2003.

RFC3912, Request for Comments: 3912, WHOIS Protocol Specification. L. Daigle. September 2004.

RFC3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, et al. January 2005.

RFC4035, Request for Comments: 4035, Protocol Modifications for the DNS Security Extensions. R. Arends, et al. March 2005.

RFC4509, Request for Comments: 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). W. Hardaker. May 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments. A. Deacon, et al. September 2007.

RFC5155, Request for Comments: 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. B. Laurie, et al. March 2008.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. D. Cooper et al. May 2008.

RFC5702, Request for Comments: 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. J. Jansen. October 2009.

RFC5890, Request for Comments: 5890, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. J. Klensin. August 2010.

RFC5952, Request for Comments: 5952, A Recommendation for IPv6 Address Text Representation. S. Kawamura, et al. August 2010.

RFC6818, Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, P. Yee. January 2013.

RFC6840, Request for Comments: 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC). S. Weiler, et al. February 2013.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. S. Santesson, et al. June 2013.

RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, et al. June 2013.

RFC7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. R. Fielding, et al. June 2014.

RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format. A. Newton, et al. March 2015.

RFC7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect). J. Reschke. April 2015.

RFC8398, Request for Comments: 8398, Internationalized Email Addresses in X.509 Certificates, MAY 2018. A. Melnikov, et al. May 2018.

RFC8499, Request for Comments: 8499, DNS Terminology. P. Hoffman, et al. January 2019.

RFC8555, Request for Comments: 8555, Automatic Certificate Management

Environment (ACME), R. Barnes et al. March 2019.

RFC8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record. P. Hallam-Baker, et al. November 2019.

RFC8738, Request for Comments: 8738, Automated Certificate Management Environment (ACME) IP Identifier Validation Extension. R.B.Shoemaker, Ed. February 2020.

RFC8823, Request for Comments: 8823, Extensions to Automatic Certificate

Management Environment for End-User S/MIME Certificates, A. Melnikov. April 2021.

RFC8954, Request for Comments: 8954, Online Certificate Status Protocol (OCSP) Nonce Extension. M. Sahni, Ed. November 2020.

RFC9495, Request for Comments: 9495, Certification Authority Authorization (CAA) Processing for Email Addresses, C. Bonnell, October 2023.

RFC9598, Request for Comments: 9598, Internationalized Email Addresses in X.509 Certificates, MAY 2018. A. Melnikov, et al. May 2024.

X.509, Recommendation ITU-T X.509 (08/2005) | ISO/IEC 9594-8:2005 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

2 Publication and Repository

2.1 Repositories

HARICA has a central data repository where policy documents, certificates of Certification Authorities and certificates of subscribers/devices are published at https://repo.harica.gr. Distributed repositories may exist for each Subordinate CA / Registration Authority that participates in the PKI.

2.2 Disclosure of Certification Authority Information

HARICA maintains a repository accessible through the Internet in which it publishes CA Certificates, CRLs, the document of Certificate Policy / Certificate Practice Statement and other documents regarding its operation (e.g. Cooperation agreements).

HARICA performs all the necessary actions for the uninterrupted – to the extent possible - availability of its repository.

The publicly accessible repository web address is https://repo.harica.gr.

Application Software Suppliers for SSL/TLS Certificates may use the following web sites for user agent verification (also available at https://testsites.harica.gr):

Root CA	Status	URL
Harica Root CA 2015	Valid	https://haricarootca2015-valid-ev.harica.gr
	Revoked	https://haricarootca2015-revoked-ev.harica.gr
	Expired	https://haricarootca2015-expired-ev.harica.gr
Harica ECC Root CA 2015	Valid	https://haricaeccrootca2015-valid-ev.harica.gr
	Revoked	https://haricaeccrootca2015-revoked-ev.harica.gr
	Expired	https://haricaeccrootca2015-expired-ev.harica.gr
Harica TLS RSA Root CA 2021	Valid	https://tls-rsa-valid-ev.root2021.harica.gr
	Revoked	https://tls-rsa-revoked-ev.root2021.harica.gr
	Expired	https://tls-rsa-expired-ev.root2021.harica.gr
Harica TLS ECC Root CA 2021	Valid	https://tls-ecc-valid-ev.root2021.harica.gr
	Revoked	https://tls-ecc-revoked-ev.root2021.harica.gr
	Expired	https://tls-ecc-expired-ev.root2021.harica.gr

2.3 Frequency of publication

CRLs are updated and published according to section 4.9.7.

2.4 Access controls on repositories

The repository section containing the certificates is publicly available through a search web page. The search is performed either by entering the certificate serial number (therefore a single certificate is returned), or by entering part of the distinguished name of the certificate subject, therefore a list of certificates is likely to be returned.

Restrictions may be applied to the repository access to protect it against enumeration attacks.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of Names

The naming rules for certificate issuance depend on the class of the certificate and comply with the ITU X.500 standard for Distinguished Names.

3.1.2 Obligation for meaningful names

The names that are included in Certificates must be related to the Subscriber. They must also be meaningful, unambiguous and produce unique DNs per Issuing CA per Subscriber. In cases where the common name (CN) or any other element would produce an ambiguous or non-unique DN per Subscriber, or where for any reason a CN is not present, HARICA will utilize a unique ID and/or serial integer in the Subject DN to identify a Certificate in a unique way.

3.1.3 Anonymity or pseudonymity of subscribers

See section 3.2.2.2.

3.1.4 Rules for interpreting various name forms

The names are composed according to the certificate type. The Subscriber's name that is composed according to the rules of the current section is called Distinguished Name (DN).

DN Attribute	Interpretation
CN or commonName (OID: 2.5.4.3)	If present, for SSL/TLS certificates, this field SHALL contain an FQDN or an IP Address that is one of the values contained in the Certificate's subjectAltName extension. For Client authentication or Code Signing certificates, this field SHALL contain a representation of the Subject's name. For S/MIME Certificates, this field shall contain values according to section 7.1.4.2.2 of the S/MIME Baseline Requirements. For non-TLS and non-S/MIME Certificates, this field is used for user-friendly representation of the Subject's name to represent itself. This name does not need to be the exact match of the fully registered organization name or the person's formal given name and surname.
G or givenName (OID: 2.5.4.42)	Subject's formal given name

SN or surname (OID: 2.5.4.4)	Subject's formal surname
E or emailAddress	Subject's email address
streetAddress (OID: 2.5.4.9)	The physical address of the Subject
postalCode (OID: 2.5.4.17)	The postal code for the physical address
L or Locality (OID: 2.5.4.7)	Postal address City
ST for State or Province Name (OID: 2.5.4.8)	Postal address State or Province
C or Country (OID: 2.5.4.6)	Subject's Country
O or Organization (OID: 2.5.4.10)	Subject's registered Organization Name. **For QEVCP-w, QEVCP-w-psd2 and EV Certificates**, the interpretation of this attribute is explained in section 7.1.4.2.1 of the EV Guidelines.
OU or Organizational Unit	Subject Organizational Unit or sub-unit, or special attribute of the signatory depending on the intended use or attributes of the certificate.
serialNumber (OID: 2.5.4.5)	A unique identifier to disambiguate the Subject Name within the context of an Issuing CA. **For QEVCP-w, QEVCP-w-psd2 and EV Certificates**, the interpretation of this attribute is explained in section 7.1.4.2.5 of the EV Guidelines
OrganizationIdentifier (OID: 2.5.4.97)	A unique identifier for the Organization
businessCategory (OID: 2.5.4.15)	**For QEVCP-w, QEVCP-w-psd2 and EV Certificates only**. This field SHALL contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of section 4.1.1.1, 4.1.1.2, 4.1.1.3 or 4.1.1.4 of the EV Guidelines, respectively.
jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3) **jurisdictionStateOrProvinceName** (OID: 1.3.6.1.4.1.311.60.2.1.2) **jurisdictionLocalityName** (OID: 1.3.6.1.4.1.311.60.2.1.1)	**For QEVCP-w, QEVCP-w-psd2 and EV Certificates only**. These fields SHALL NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. The interpretation of this attribute is explained in section 7.1.4.2.4 of the EV Guidelines

3.1.4.1 End-Entity Certificates for electronic signatures

Certificates for Advanced or Qualified electronic signatures are issued to natural persons and include at least the following attributes in the Certificate subject DN:

- "commonName"
- "givenName" and/or[3] "surname"
- "countryName"

3.1.4.2 End-Entity Certificates for electronic seals

Certificates for Advanced or Qualified electronic seals are issued to legal entities and include at least the following attributes in the Certificate subject DN:

- "commonName"
- "organizationName"
- "countryName"
- "organizationIdentifier"

3.1.4.3 End-Entity Certificates for SSL/TLS usage

Certificates for SSL/TLS under the DVCP, must include at least one FQDN or IP Address in the `subjectAltName` extension. The `commonName` field is optional but if it is present, it must contain at least one FQDN or an IP address that is one of the values contained in the `subjectAltName` extension.

Certificates for SSL/TLS under the OVCP, in addition to the above fields, they shall include at least the following attributes in the Certificate subject DN:

- "organizationName"
- "countryName"
- "localityName" and/or "stateOrProvinceName".

Certificates for SSL/TLS under the QNCP-w or QNCP-w-gen policy per ETSI EN 319 411-2, if they are issued to a legal entity, shall include at least the following attributes in the Certificate subject DN:

- "organizationName"
- "countryName"
- "localityName" and/or "stateOrProvinceName"
- “organizationIdentifier”

and shall contain a QCStatement extension per ETSI EN 319 412-1. Certificates for PSD2 and Open Banking shall include extensions per ETSI TS 119 495.

Certificates for SSL/TLS under the QNCP-w policy per ETSI EN 319 411-2, if they are issued to a natural person, they shall include at least the following attributes in the Certificate subject DN:

- "givenName" and/or “surname” (if the natural person carries only one official name, it is allowed to include one of the two attributes)
- "countryName"
- "localityName" and/or "stateOrProvinceName"

and shall contain a QCStatement extension per ETSI EN 319 412-1.

[3] The option “givenName or surname” is to accommodate rare cases of Natural Persons with only one value (givenName or surname) in the official identity proofing document.

Certificates for SSL/TLS under the EV Guidelines, shall include at least the following attributes in the Certificate subject DN:

- "organizationName"
- "countryName"
- "localityName" and/or "stateOrProvinceName"
- “serialNumber”
- “businessCategory”
- “jurisdictionCountryName” and/or “jurisdictionStateOrProvinceName” and/or “jurisdictionLocalityName”.

Certificates for SSL/TLS under the EVCP and QEVCP-w policies per ETSI EN 319 411-1 and 319 411-2, in addition to the above fields, they shall include at least the following additional attribute in the Certificate subject DN:

- “organizationIdentifier”

and shall contain a QCStatement extension per ETSI EN 319 412-1.

Certificates for SSL/TLS and eSeal under the QEVCP-w-psd2 and QCP-l-psd2 policies, shall include at least the following additional attribute in the Certificate subject DN:

- “organizationIdentifier”

and shall contain a PSD2 QCStatement that includes the NCA identifier and the PSP roles of the subject per ETSI TS 119 495.

3.1.4.4 End-Entity Certificates for Code Signing

Certificates for code signing under the IVCP or OVCP issued to natural persons or legal entities respectively, include at least the following attributes in the Certificate subject DN:

- "commonName"
- "organizationName". Because Subject name attributes for natural persons "givenName" and "surname" are not broadly supported by application software, HARICA may use the subject:organizationName field to convey a natural person Subject’s name or DBA.
- "CountryName"

Certificates for EV code signing under the EVCP, in addition to the above fields, Certificates shall include at least the following additional attributes in the Certificate subject DN:

- “serialNumber”
- “businessCategory”
- “jurisdictionCountryName” and/or “jurisdictionStateOrProvinceName” and/or “jurisdictionLocalityName”,
- "localityName" and/or "stateOrProvinceName"

according to section 7.1.4.2 of the EV Guidelines.

3.1.4.5 End-Entity Certificates for Web Client Authentication

Certificates for web client authentication issued to natural persons or legal entities, include at least the following attributes in the Certificate subject DN:

- "commonName"
- "organizationName". Because Subject name attributes for natural persons "givenName" and "surname" are not broadly supported by application software, HARICA may use the subject:organizationName field to convey a natural person Subject's name or DBA
- "countryName".

3.1.5 Uniqueness of names

The Distinguished Name in each Subscriber Certificate must be unique for each Issuing CA, while it is desirable to be unique in the entire HARICA hierarchy.

3.1.6 Resolution Process regarding disputes about naming property rights and the role of trademarks

Applicants represent and warrant, by submitting a certificate request that their request is clear from any third-party intellectual property or proprietary rights, does not contain data which in any way interferes with or infringes upon the rights of any third party in any jurisdiction with respect to patents, trademarks, service marks, trade names, company names, "doing business as" (DBA) names and other trade rights, and does not present the data for any unlawful purpose whatsoever. Data covered by this representation and warranty includes but is not limited to any domain name, domain name space, Distinguished Name (DN), or Fully-Qualified Domain Name (FQDN), and/or any trade name or DBA name, contained in any part of the certificate request.

The regulatory body for matters concerning disputes about naming property rights or about the provisioning of the services or any related matters, is the HARICA PMC. See also section 9.13.

3.2 Initial identity validation

Under the current verification policy, HARICA shall only require identity evidence sufficient to satisfy the requirements of the intended certificate type. HARICA issues a variety of types of digital certificates, intended for SSL/TLS, S/MIME, Code Signing, Digital Signatures. Each certificate type has different levels of assurance depending on the validation policy level which start from LCP up to Extended Validation and QCP.

HARICA shall inspect any document relied upon for verification, for alteration or falsification. HARICA shall verify the identity and status of any Applicant as appropriate and required for the certificate type and assurance level requested. Alteration or falsification of any document used in this process, misrepresentation of the identity or status of any Applicant referenced in this process, shall constitute grounds for disapproval of a certificate request and/or immediate revocation of any existing certificate relying upon altered or falsified documents or false or misrepresented identity or status according to section 4.9.1.1.

3.2.1 Method to prove possession of private key

Initially, the identity of the Applicant is verified and a CSR is submitted that contains the Public Key of the corresponding Private Key. The CSR establishes that the Applicant possesses the Private Key that is associated to the Public Key to be included in the requested certificate, since the CSR contains a signature created by the Private Key.

For Qualified Certificates associated with private keys in a Qualified Signature/Seal Creation Device (QSCD), in accordance with European/Greek Electronic Signature law, private keys are generated in Qualified Signature Creation Devices in the presence of the Certificate Holder and an authorized member of the RA that certifies that the private key is created in the QSCD. The presence of an RA authorized member can be skipped if there is a certified procedure that ensures by technical means, that the Applicant's private key is generated in the QSCD. The Certificate owner is responsible for securing the QSCD with a Personal Identification Number (PIN).

This requirement does not apply when a Key Pair is generated by HARICA on behalf of a Subscriber for Qualified Signatures/Seals, Code Signing and EV Code Signing Certificate Applicants. In these cases, HARICA shall implement controls to generate the keys in special-purpose crypto devices meeting the requirements of section 6.2.7.4 and delivering these devices securely to the Subscriber.

3.2.2 Authentication of organization identity

The Registration Authority must confirm that the Applicant belongs to the Organization, the name of which is included in the certificate. When an Applicant requests a Certificate as a Legal Entity (under the QCP-l or QCP-l-qscd policy), then the Applicant's Representative must provide the necessary documentation including the Legal Entity's complete name, legal status as well as relevant Country/State/City-level registration/incorporating information. The Applicant must also provide documentation that affirms the right to represent the organization. All this information must be verified by a HARICA Validation Specialist.

Each Legal Entity must have its own authorized requestors and a Parent Company cannot authorize Certificate applications for Subsidiary Companies.

When an RA receives a "High Risk Certificate Request" which matches a domain or Organization flagged as "high risk", additional scrutiny and verification is performed prior to issuance.

HARICA also checks whether the Applicant, Contract Signer, or Certificate Approver is on a denied persons list published by the Greek government, if any.

If a Delegated Third Party fulfills any of HARICA's obligations under this section, HARICA SHALL verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as HARICA's own processes.

The verification of organization identity SHALL follow the EV verification procedures described in the EV Guidelines, before issuing an EV Certificate.
HARICA SHALL ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of EV Guidelines and matches the information confirmed and documented by HARICA pursuant to its verification processes.

HARICA SHALL only issue EV Certificates to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity following the requirements of sections 4.1.1.1 to 4.1.1.4 of the EV Guidelines.

HARICA discloses the Incorporating or Registration Agencies used for validating Organization Identities at the HARICA repository as described in section 2.1, prior to issuance of the EV certificate.

3.2.2.1 Identity

If the Certificate's SubjectDN is to include the name or address of an organization, the RA shall verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. HARICA shall verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

- A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
- A third-party database that is periodically updated and considered a Reliable Data Source as defined in section 3.2.2.7;
- A site visit by HARICA or a third party who is acting as an agent for HARICA; or
- An Attestation Letter.

HARICA may verify **the address of the Applicant** (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other reliable form of identification.

For the issuance of EV Certificates, HARICA SHALL verify the following:

- The Applicant's legal existence and identity, as per Section 3.2.2 of the EV Guidelines,
- The Applicant's physical existence (business presence at a physical address), as per Section 3.2.4 of the EV Guidelines,
- The Applicant's operational existence (business activity), as per Section 3.2.6 of the EV Guidelines, and
- A Verified Method of Communication with the entity to be named as the Subject in the Certificate, as per Section 3.2.5 of the EV Guidelines.

For Non-Latin Organization Names, Romanized Names, Translated Names and Organizations incorporated in Japan HARICA conforms to the requirements of EV Guidelines Appendix D.

3.2.2.1.1 Legal Entity Identifier

For Legal Entities, HARICA may include a Legal Entity Identifier (LEI), as provided by the Global Legal Entity Identifier Foundation (GLEIF), if the entity has been "fully corroborated" (Corroboration Level="FULLY_CORROBORATED"). HARICA shall bind the LEI with the Legal Entity described in the Subject of the Certificate after it has established the identity via means described in section 3.2.2.1. LEI is treated as additional correlation of identity information found in the certificate.

3.2.2.2 DBA/Tradename/Roles

HARICA does not allow certificate issuance for anonymous users. The certificate issuance for pseudonyms e.g. "Rector" or "President" is not provided in the present Certification Practice Statement but also it is not prohibited. These pseudonyms should be included as extra information in the digital certificates after appropriate validation with information that proves that the actual person holds the corresponding pseudonym/role. E.g. for the "Supervisor" role, there must be a document proving that the subject of the certificate is entitled to this role.

If the Certificate's subject DN is to include a DBA or tradename, HARICA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or trade names;
4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that HARICA determines to be reliable.

For the issuance of EV Certificates, HARICA SHALL verify the Applicant's assumed name, as per Section 3.2.3 of the EV Guidelines.

3.2.2.3 Verification of Country

If the `subject:countryName` field is present, then HARICA shall verify the country associated with the Subject using one of the following:

- the IP Address range assignment by country for either
  - the web site's IP address, as indicated by the DNS record for the web site or
  - the Applicant's IP address;
- the ccTLD of the requested Domain Name;

- information provided by the Domain Name Registrar; or
- a method identified in sections 3.2.2.1 or 3.2.3.1.

3.2.2.4 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

HARICA SHALL confirm that prior to issuance, each Fully-Qualified Domain Name (FQDN) listed in the Certificate has been validated as follows:

1. When the FQDN is not an Onion Domain Name, HARICA SHALL validate the FQDN using at least one of the methods listed in this section 3.2.2.4; and
2. When the FQDN is an Onion Domain Name, HARICA SHALL validate the FQDN in accordance with ANNEX E Issuance of Certificates for Onion Domain Names.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated within the time period specified in section 4.2.1, prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, Affiliate or the Applicant as an individual Natural Person.

For the issuance of EV Certificates, HARICA SHALL verify that the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate, as per Section 3.2.7 of the EV Guidelines.

DNSSEC validation back to the IANA DNSSEC root trust anchor SHALL be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective SHALL:

- perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- support NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handle the security concerns enumerated in RFC 6840 Section 4.

HARICA SHALL NOT use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

For e-mail Domain Validation methods described in sections 3.2.2.4.4, 3.2.2.4.13, 3.2.2.4.14, DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS CNAME, CAA, TXT queries attempting to obtain the Authorization Domain Name associated with the validation of domain authorization or control by the Primary Network Perspective. For all other DNS queries, DNSSEC validation back to the IANA DNSSEC root trust anchor SHOULD be performed.

For all other Domain Validation methods, DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in 8.7.

HARICA shall maintain a record of which domain validation method was used to validate each domain, including the relevant CA/B Forum Baseline Requirements version number applicable.

Note: FQDNs may be listed in Subscriber Certificates using *dNSNames* in the *subjectAltName* extension or in Subordinate CA Certificates via *dNSNames* in *permittedSubtrees* within the *Name Constraints* extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method has been retired and SHALL NOT be used.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

This method has been retired and SHALL NOT be used.

3.2.2.4.3 Phone Contact with Domain Contact

This method has been retired and SHALL NOT be used.

3.2.2.4.4 Email to a Constructed Address

Confirming the Applicant's control over the requested FQDN by

1. 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,
2. including a Random Value in the email, and
3. Receiving a confirming response utilizing the Random Value.

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 Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than thirty (30) days from its creation.

Note: Once the FQDN has been validated using this method, HARICA 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.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2028: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.4.5 Domain Authorization Document

This method has been retired and SHALL NOT be used.

3.2.2.4.6 Agreed-Upon Change to Website

This method has been retired and SHALL NOT be used.

3.2.2.4.7 DNS Change

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

1. an Authorization Domain Name or
2. an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character.

i. If a Random Value is used, HARICA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value afterthirty (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).

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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.

If HARICA or an Affiliate of HARICA operates a DNS zone to which Applicants can delegate (via CNAME) their underscore-prefixed Domain Label, HARICA MUST ensure that each Applicant delegates to a unique FQDN within that zone. HARICA or Affiliate of HARICA SHOULD NOT operate such a service, and SHOULD direct any Applicants using such a service to use the method described in Section 3.2.2.4.22 instead.

Note: Once the FQDN has been validated using this method, HARICA 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

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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, HARICA MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless HARICA performs a separate validation for that FQDN using another allowed method as described in section 3.2.2.4. This method is NOT suitable for validating Wildcard Domain Names.

Effective March 15, 2026: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.4.9 Test Certificate

This method has been retired and SHALL NOT be used.

3.2.2.4.10 TLS Using a Random Value

This method has been retired and SHALL NOT be used.

3.2.2.4.11 Any Other Method

This method has been retired and SHALL NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if HARICA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

When issuing Subscriber Certificates, the CA MUST NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period.

When obtaining Domain Contact information for a requested Domain Name the CA:

- if using the WHOIS protocol (RFC 3912), MUST query IANA's WHOIS server and follow referrals to the appropriate WHOIS server.
- if using the Registry Data Access Protocol (RFC 7482), MUST utilize IANA's bootstrap file to identify and query the correct RDAP server for the domain.
- MUST NOT rely on cached 1) WHOIS server information that is more than 48 hours old, or 2) RDAP bootstrap data from IANA that is more than 48 hours old, to ensure that it relies upon up-to-date and accurate information.

Note: Once the FQDN has been validated using this method, HARICA 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.

3.2.2.4.13 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value SHALL be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set SHALL be 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 SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than thirty (30) days from its creation.

Note: Once the FQDN has been validated using this method, HARICA 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.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2028: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.4.14 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value SHALL be 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 SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than thirty (30) days from its creation.

Note: Once the FQDN has been validated using this method, HARICA 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.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2028: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.4.15 Phone Contact with Domain Contact v2

This method has been retired and SHALL NOT be used.

3.2.2.4.16 Phone Contact with DNS TXT Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the Authorization Domain Name. Each phone call MAY confirm control of multiple Authorization Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each Authorization Domain Name being verified and they provide a confirming response for each Authorization Domain Name.

HARICA SHALL NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, HARICA may leave the Random Value and the Authorization Domain Name(s) being validated. The Random Value SHALL be returned to HARICA to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than thirty (30) days from its creation.

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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, HARICA 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.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set SHALL be found using the search algorithm defined in RFC 8659 section 3.

HARICA SHALL NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, HARICA may leave the Random Value and the ADN(s) being validated. The Random Value SHALL be returned to HARICA to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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, HARICA 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.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

1. The entire Request Token or Random Value SHALL NOT appear in the request used to retrieve the file, and
2. HARICA SHALL receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Value:

1. SHALL be located on the Authorization Domain Name, and
2. SHALL be located under the "/.well-known/pki-validation" directory, and
3. SHALL be retrieved via either the "http" or "https" scheme, and
4. SHALL be accessed over an Authorized Port.

HARICA follows redirects and the following apply:

1. Redirects SHALL be initiated at the HTTP protocol layer. Redirects SHALL be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, section 3. Redirects SHALL be to the final value of the Location HTTP response header, as defined in RFC 7231, section 7.1.2.
2. Redirects SHALL be to resource URLs with either the "http" or "https" scheme.
3. Redirects SHALL be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. HARICA SHALL provide a Random Value unique to the certificate request.
2. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Except for Onion Domain Names, HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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: HARICA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless HARICA performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

HARICA SHALL receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, section 8.3) SHALL NOT be used for more than 30 days from its creation.

HARICA follows redirects and the following apply:

1. Redirects SHALL be initiated at the HTTP protocol layer. Rredirects SHALL be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, section 3. Redirects SHALL be to the final value of the Location HTTP response header, as defined in RFC 7231, section 7.1.2.
2. Redirects SHALL be to resource URLs with either the "http" or "https" scheme.
3. Redirects SHALL be to resource URLs accessed via Authorized Ports.

Except for Onion Domain Names, HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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: HARICA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless HARICA performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.20 TLS Using ALPN

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The following are additive requirements to RFC 8737.

The token (as defined in RFC 8737, Section 3) MUST NOT be used for more than 30 days from its creation.

Except for Onion Domain Names, HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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: HARICA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless HARICA performs separate validations for each of those other FQDNs using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.21 DNS Labeled with Account ID - ACME

Confirming the Applicant's control over the FQDN by performing the procedure documented for a "dns-account-01" challenge in draft 00 of "Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge," available at https://datatracker.ietf.org/doc/draft-ietf-acme-dns-account-label/.

The token (as defined in draft 00 of "Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge," Section 3.1) MUST NOT be used for more than 30 days from its creation.

HARICA MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same token as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, HARICA 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.

3.2.2.4.22 DNS TXT Record with Persistent Value

Confirming the Applicant's control over a FQDN by verifying the presence of a Persistent DCV TXT Record identifying the Applicant. The record MUST be placed at the "`_validation-persist`" label prepended to the Authorization Domain Name being validated (i.e., "`_validation-persist.[Authorization Domain Name]`"). For this method, HARICA MUST NOT use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. This prohibition overrides the Authorization Domain Name definition. CNAME records MAY be followed when resolving the Persistent DCV TXT Record.

HARICA MUST confirm the Persistent DCV TXT Record's RDATA value fulfills the following requirements:

1. The RDATA value MUST conform to the `issue-value` syntax as defined in RFC 8659, Section 4.2; and
2. The `issuer-domain-name` value MUST be an Issuer Domain Name disclosed by HARICA in Section 4.2.4; and
3. The `issue-value` MUST contain an `accounturi` parameter, where the parameter value is a unique URI (as described by RFC 8657, Section 3) identifying the account of the Applicant which requested validation for this FQDN; and

4. The `issue-value` MAY contain a `persistUntil` parameter. If present, the parameter value MUST be a base-10 encoded integer representing a UNIX timestamp (the number of seconds since 1970-01-01T00:00:00Z ignoring leap seconds); and
5. The `issue-value` MAY contain additional parameters. HARICA SHALL ignore any unknown parameter keys.

If the `persistUntil` parameter is present, HARICA MUST evaluate its value. If the time of the check is after the time specified in the `persistUntil` parameter value, HARICA MUST NOT use the record as evidence of the Applicant's control over the FQDN.

For example, the Persistent DCV TXT Record might look like:

```
_validation-persist.example.com IN TXT "authority.example;
accounturi=https://authority.example/acct/123;
persistUntil=1782424856"
```

For the purposes of Section 4.2.1, HARICA MUST consider 10 days as the maximum validation data reuse period for validations completed using this method.

The following table shows how the `persistUntil` parameter affects whether a DNS record can be used for validation at different points in time:

Date/time of validation	persistUntil	Usable for validation	Explanation
2025-06-15T12:00:00Z	2026-01-01T00:00:00Z (1767225600)	Yes	Validation time is before persistUntil timestamp, so record is usable
2025-06-15T12:00:00Z	2025-01-01T00:00:00Z (1735689600)	No	Validation time is after persistUntil timestamp, so record is not usable
2025-06-15T12:00:00Z	(not present)	Yes	No persistUntil parameter present, so no time restriction applies

Table 1: Examples of how the persistUntil parameter affects validation

HARICA MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe a Persistent DCV TXT Record that demonstrates the Applicant's control over the domain and contains the same `accounturi` parameter as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, HARICA 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.

3.2.2.5 Authentication for an IP Address

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.

HARICA SHALL confirm that, prior to issuance, each IP Address listed in the Certificate has been validated using at least one of the methods specified in this section.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as section 4.2.1 of this CP/CPS) prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

HARICA SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

Note: IP Addresses verified in accordance with this section may be listed in Subscriber Certificates as defined in section 7.1.4 or in Subordinate CA Certificates via iPAddress in permittedSubtrees within the Name Constraints extension. HARICA is not required to verify IP Addresses listed in Subordinate CA Certificates via iPAddress in excludedSubtrees in the Name Constraints extension prior to inclusion in the Subordinate CA Certificate.

3.2.2.5.1 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by HARICA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value SHALL NOT appear in the request.

If a Random Value is used, HARICA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) thirty (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 this CP/CPS).

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value SHALL be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

HARICA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

HARICA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than thirty (30) days from its creation.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.5.3 Reverse Address Lookup

Confirming the Applicant’s control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under section 3.2.2.4.

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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.

Effective March 15, 2027: HARICA SHALL NOT rely on this method. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.5.4 Any Other Method

Not used.

3.2.2.5.5 Phone Contact with IP Address Contact

Confirming the Applicant's control over the IP Address by calling the IP Address Contact’s phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. HARICA SHALL place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to a single number.

In the event that someone other than an IP Address Contact is reached, HARICA MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, HARICA may leave the Random Value and the IP Address(es) being validated. The Random Value SHALL be returned to HARICA to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than thirty (30) days from its creation.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - HARICA SHALL NOT rely on this method. - Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue Subscriber Certificates.

3.2.2.5.6 ACME "http-01" method for IP Addresses

Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in RFC 8738.

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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.

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in RFC 8738.

HARICA SHALL implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. 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.

3.2.2.5.8 DNS TXT Record with Persistent Value in the Reverse Namespace

Confirming the Applicant's control over the IP Address by converting the IP address to a Reverse Zone Domain Name and then verifying the presence of a Persistent DCV TXT Record identifying the Applicant as defined in Section 3.2.2.4.22. The record MUST be placed at the "`_ip-validation-persist`" label prepended to the Reverse Zone Domain Name of the IP address being validated (i.e., "`_ip-validation-persist.[Reverse Zone Domain Name]`").

3.2.2.6 Wildcard Domain Validation

Before issuing a Wildcard Certificate, HARICA follows a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is "registry-controlled" or is a "public suffix" (e.g. "*.com", "*.co.uk"). This is done by regularly retrieving and consulting a "public suffix list" such as https://publicsuffix.org/ (PSL).

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", HARICA SHALL refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. HARICA SHALL NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

Wildcard Certificates are not allowed for EV SSL/TLS Certificates unless the FQDN portion of the Wildcard Domain Name is an Onion Domain Name verified in accordance with ANNEX E Issuance of Certificates for Onion Domain Names.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, HARICA shall evaluate the source for its reliability, accuracy and resistance to alteration or falsification. HARICA considers the following criteria for its decision whether or not to accept data from a Data Source:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

HARICA uses Academic/Research Institutions, Official Directory Services to verify identities and roles within the Academic/Research Community.

HARICA shall ensure that, prior to the use of an Incorporating Agency or Registration Agency to fulfill these verification requirements, the Incorporating Agency or Registration Agency data sources used for EV Certificates will be publicly disclosed in the repository described in section 2.1.

This Agency Information SHALL include at least the following:

- Sufficient information to unambiguously identify the Incorporating Agency or Registration Agency (such as a name, jurisdiction, and website); and,
- The accepted value or values for each of the `subject:jurisdictionLocalityName` (OID: 1.3.6.1.4.1.311.60.2.1.1), `subject:jurisdictionStateOrProvinceName` (OID: 1.3.6.1.4.1.311.60.2.1.2), and `subject:jursidictionCountryName` (OID: 1.3.6.1.4.1.311.60.2.1.3) fields, when a certificate is issued using information from

that Incorporating Agency or Registration Agency, indicating the jurisdiction(s) that the Agency is appropriate for; and,

- A revision history that includes a unique version number and date of publication for any additions, modifications, and/or removals from this list.

3.2.2.7.1 Qualified Independent Information Source

A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if HARICA determines that:

(1) Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and

(2) The database provider updates its data on at least an annual basis.

HARICA uses a documented process to check the accuracy of the database and ensures its data is acceptable, including reviewing the database provider's terms of use. HARICA SHALL NOT use any data in a QIIS that HARICA knows is (i) self-reported and (ii) not verified by the QIIS as accurate. Databases in which HARICA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities or subcontractors to whom HARICA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest, do not qualify as a QIIS.

3.2.2.7.2 Qualified Government Information Source

A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. The use of third-party vendors to obtain the information from the Government Entity is allowed, provided that the third party obtains the information directly from the Government Entity.

3.2.2.7.3 Qualified Government Tax Information Source

A Qualified Government Tax Information Source is a Qualified Government Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. TAXIS in Greece, the IRS in the United States).

3.2.2.8 CAA Records

As part of the Certificate issuance process, HARICA SHALL retrieve and process CAA records in accordance with RFC 8659 for each `dNSName` in the `subjectAltName` extension that does not contain an Onion Domain Name.

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see Section 3.2.2.4) or IP address(es) (see Section 3.2.2.5) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 3.2.2.9). To

corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, HARICA MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

When processing CAA records, HARICA SHALL process the `issue`, `issuewild`, and `iodef` property tags as specified in RFC 8659, and SHALL process the `issuemail` property tag as specified in RFC 9495, although it is not required to act on the contents of the `iodef` property tag. Additional property tags MAY be supported, but SHALL NOT conflict with or supersede the mandatory property tags set out in this document. HARICA SHALL respect the critical flag and not issue a certificate if it encounters an unrecognized property tag with this flag set.

If HARICA issues, it SHALL do so within the TTL of the CAA record, or 8 hours, whichever is greater. This stipulation does not prevent HARICA from checking CAA records at any other time.

HARICA MAY treat a non-empty CAA RRset that does not contain any `issue` property tags (and also does not contain any `issuewild` property tags when performing CAA processing for a Wildcard Domain Name) as permission to issue, provided that no records in the CAA RRset otherwise prohibit issuance.

CAA checking is optional:

- for certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked
- for certificates issued by a Technically Constrained Subordinate CA as set out in section 7.1.5 where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

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

- the failure is outside HARICA’s infrastructure; and
- the lookup has been retried at least once; and
- HARICA has confirmed that the domain is “Insecure” as defined in RFC 4035 Section 4.3.

DNSSEC validation back to the IANA DNSSEC root trust anchor SHALL be performed on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective SHALL:

- perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- support NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handle the security concerns enumerated in RFC 6840 Section 4.

HARICA SHALL NOT use local policy to disable DNSSEC validation on any DNS query associated with CAA record lookups.

DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) SHALL NOT be treated as permission to issue.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

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.

HARICA MAY 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 SHALL provide HARICA with the necessary information to allow it to affirmatively assess:

a. the presence of the expected
    i. Random Value,
    ii. Request Token,
    iii. IP Address, or
    iv. Contact Address,
    v. Persistent DCV TXT Record,
    as required by the relied upon validation method specified in Sections 3.2.2.4 and 3.2.2.5; and
b. HARICA's authority to issue to the requested domain(s), as specified in Section 3.2.2.8.

Sections 3.2.2.4 and 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 SHALL NOT be 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 HARICA SHALL 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 SHALL 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 DNS resolvers SHALL 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.

HARICA MAY immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., HARICA can immediately retry validation using "Email to DNS TXT Contact" if "Agreed-Upon Change to Website - ACME" does not corroborate the outcome of Multi-Perspective Issuance Corroboration). When retrying Multi-Perspective Issuance Corroboration, HARICA SHALL NOT rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If HARICA does not rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements SHALL 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 them 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.

HARICA 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.

Table 2 Quorum Requirements

Distinct Remote Network Perspectives Used	Allowed non-Corroborations
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration:

MUST:

- Network Hardening
    - Rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the

global Internet routing system for providing internet connectivity to the Network Perspective.

SHOULD:

- Facility & Service Provider Requirements
    - Be hosted from an ISO/IEC 27001 certified facility or equivalent security framework independently audited and certified or reported.
    - Rely on services covered in one of the following reports: System and Organization Controls 2 (SOC 2), ISAE 3000, ENISA 715, FedRAMP Moderate, C5:2020, CSA STAR CCM, or equivalent services framework independently audited and certified or reported.
- Vulnerability Detection and Patch Management
    - Implement intrusion detection and prevention controls to protect against common network and system threats.
    - Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
    - Undergo or perform a Vulnerability Scan at least every three (3) months.
    - Undergo a Penetration Test on at least an annual basis.
    - Apply recommended security patches within six (6) months of the security patch's availability, unless HARICA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.
- System Hardening
    - Disable all accounts, applications, services, protocols, and ports that are not used.
    - Implement multi-factor authentication for all user accounts.
- Network Hardening
    - Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications identified as necessary to its operations.
    - Rely upon networks (e.g., Internet Service Providers) that: 1) use mechanisms based on Secure Inter-Domain Routing (RFC 6480), for example, BGP Prefix Origin Validation (RFC 6811), 2) make use of other non-RPKI route-leak prevention mechanisms (such as RFC 9234), and 3) apply current best practices described in BCP 194. While It is RECOMMENDED that under normal operating conditions Network Perspectives performing Multi-Perspective Issuance Corroboration forward all Internet traffic via a network or set of networks that filter RPKI-invalid BGP routes as defined by RFC 6811, it is NOT REQUIRED.

Beyond the above considerations, computing systems performing Multi-Perspective Issuance Corroboration are considered outside of the audit scope described in Section 8 of this CP/CPS.

If any of the above considerations are performed by a Delegated Third Party, HARICA MAY obtain reasonable evidence from the Delegated Third Party to ascertain assurance that one or more of the above considerations are followed. As an exception to Section 1.3.2, Delegated Third Parties are not required to be within the audit scope described in Section 8 of this CP/CPS to satisfy the above considerations.

Phased Implementation Timeline:

- **Effective March 15, 2025,** HARICA SHALL implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. HARICA MAY proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.
- **Effective September 15, 2025,** HARICA SHALL implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. HARICA SHALL ensure that the requirements defined in Quorum Requirements Table are satisfied. If the requirements are not satisfied, HARICA SHALL NOT proceed with issuance of the Certificate.
- **Effective March 15, 2026,** HARICA SHALL implement Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. HARICA SHALL ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then HARICA SHALL NOT proceed with issuance of the Certificate.
- **Effective June 15, 2026,** HARICA SHALL implement Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives. HARICA SHALL ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then HARICA SHALL NOT proceed with issuance of the Certificate.
- **Effective December 15, 2026,** HARICA SHALL implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. HARICA SHALL ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then HARICA SHALL NOT proceed with issuance of the Certificate.

3.2.3 Authentication of individual person identity

If an Applicant is a natural person, then HARICA SHALL verify the Applicant’s name, Applicant’s address, and the authenticity of the certificate request.

For a certificate capable of being used for digitally signing or encrypting email messages (S/MIME Certificate), HARICA shall follow the procedures described in section 3.2.2 of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates", to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf.

HARICA MAY rely on validation performed for an Authorization Domain Name as being valid for subdomains of that Authorization Domain Name using the domain validation methods described in section 3.2.2.4.

3.2.3.1 Entity applying for a user certificate

Applicants that request personal certificates by HARICA must prove their identity. There are two classes of personal certificates. "Class A" refers to certificates whose corresponding private keys are generated and reside in a Qualified Signature/Seal Creation Device (QSCD) and are issued under the presence of authorized personnel of the RA verifying that the private key is actually generated in the QSCD.

Possible Policy Identifiers for "Class A" Certificates are:

- NCP+
- QCP-n-qscd
- QCP-l-qscd
- QCP-l-psd2-qscd
- Code Signing
- EV Code Signing

"Class B" refers to certificates whose private keys are generated using software. Possible Policy Identifiers for "Class B" Certificates are:

- LCP
- NCP
- QCP-n
- QCP-l
- QCP-l-psd2

The central Registration Authority may also rely on Affiliated Institutions for Identity Validation of Applicants affiliated with Greek Academic and Research Institutions. These institutions act as Enterprise RAs and use secure authentication ways in order to verify the identity of Applicants. The affiliated institutions are compelled to have certified the identity of a user via physical presence, by means of an official document that bears the photograph of the beneficiary (e.g. police identity, passport, driving license). Alternatively, the Central RA can execute the above process for any Applicant requesting a user certificate.

If an Academic and Research Institution that an Applicant belongs to, has already performed a procedure to verify the Applicant's physical identity in the past (e.g. for the provision of an Institutional Electronic User Account or email address), there is no need to repeat the procedure but a typical confirmation through the officially certified email address of the user is considered sufficient.

HARICA's central RA uses the following methods for identity, email ownership and control verification:

i. Simple email verification. The Applicant enters the email address at the initial certificate request form and a verification email is sent back with a link to a unique web page. After following this link, an email is sent to the corresponding Institution's authorized "Validator" that requires an approval based on the full name entered by the Applicant and the Applicant's email. This approval requires the identification of the user with his/her physical presence and an acceptable official document. If this procedure took place before (e.g. for the creation of an email account) then there is no reason to be repeated.
ii. LDAP server. The Applicant enters the personal email address at the initial certificate request form and the corresponding institutional password. This information is verified against the institution's LDAP server. If the verification is successful, the verified real name of the user is retrieved from the official institutional LDAP server and a certificate request is generated. In order for a user to be listed in the institutional directory server, the institution must have verified the user with his/her physical presence and an acceptable official photo-id document.
iii. Single Sign On (SSO) architecture based on the SAML specification. The Applicant enters the personal email address at the initial request form and is then redirected to the corresponding Identity Provider. The Identity Provider verifies the user and returns the verified real name and the email address of the Applicant as attributes to the Registration Authority. In order for an Applicant to be eligible for validation by the Identity Provider of an institution, the institution must have verified the user with his/her physical presence and an acceptable official photo-id document.
iv. Physical presence. If an individual fails to use the previous methods, he/she may physically appear at the central RA. The RA must verify the Applicant's name, address and the authenticity of the certificate request. HARICA SHALL verify the Applicant's name using at least one legible copy, which discernibly shows the Applicant's face, of a currently valid government-issued photo ID (passport, driver's license, academic ID, national ID, or equivalent document type). HARICA SHALL inspect the copy for any indication of alteration or falsification. HARICA SHALL verify the Applicant's address using a reliable form of identification such as a government ID, utility bill, bank or credit card statement. HARICA SHALL verify the ownership of an email address by performing a challenge-response procedure according to "Simple email verification" method (i) listed above.

"Class A" Certificates should include an extra organizational unit (OU) in the subject field with the value "Class A – Private Key created and stored in hardware CSP". Additionally, Certificates for Qualified electronic signatures/seals SHALL include the OID `id-etsi-qcs-QcSSCD` at the `qcStatements` extension. Class A certificates are fully compliant with the Qualified Signature/Seal Creation Devices (QSCD) definition, per eIDAS.

"Class B" Certificates should to include an extra organizational unit (OU) in the subject field with the value "Class B – Private Key created and stored in software CSP".

3.2.3.1.1 Validation for Qualified Certificates

For the issuance of Qualified Certificates according to eIDAS, identity of natural or legal persons is verified according to Article 24 paragraph 1 options (a) – (d).

(a) The Applicant shall physically appear at a HARICA RA or properly authorized national authority. The RA must verify the Applicant's name. HARICA SHALL verify the Applicant's name using at least one legible copy, which discernibly shows the Applicant's face, of a currently valid government-issued photo ID (passport, driver's license, national ID, or equivalent document type). HARICA SHALL inspect the copy for any indication of alteration or falsification.
(b) The Applicant shall be authenticated via nationally-issued electronic identification (eID). This option is allowed only if the Applicant's National eID scheme is "Notified" and the Level of Assurance is marked as "High".
(c) The Applicant shall use an existing Qualified Electronic Signature Certificate to digitally sign a HARICA application form. HARICA shall ensure that the signing certificate was issued in compliance with point (a) or (b).
(d) HARICA has implemented the provisions of the Ministerial Decision 27499/2021-08 for Remote Identity Proofing in accordance with eIDAS Article 24 paragraph 1 option (d). The list of acceptable identity proofing documents for the remote process shall be published in the Repository described in section 2.1. Two (2) options have been implemented to support remote identity proofing which has been certified as providing equivalent assurance in terms of reliability to physical presence.
    i. Synchronous identity proofing via real-time teleconference with a Validation Specialist.
    ii. Asynchronous identity proofing via remote videoconference/dynamic selfie and agent review at a later stage. During the remote videoconference session, several security controls are in place such as face recognition, liveliness tests, identity proofing document verification and applicant consent. A Validation Specialist examines the application at a later stage, after the completion of the videoconference.

3.2.3.2 Individual who applies for a device certificate

An Applicant who is in control of a device/server, must either possess a certificate issued by HARICA or authentication credentials provided during initial registration.

The Applicant submits the application for a device certificate after proper authentication.

HARICA verifies device ownership. For SSL/TLS certificates used for domains belonging to Academic/Research institutions, a verification email is sent to the corresponding Institution's authorized "Validator" who verifies the validity of the FQDN of the certificate request. The Institution network administrator also verifies that the person who applied for the certificate is the rightful administrator of the server using the FQDN according to the institution's database of users / servers.

In addition to the above-mentioned procedure, HARICA's central RA performs verification methods listed in section 3.2.2.4.

3.2.4 Non verified subscriber information

The certificates that are issued do not include non-verified subscriber information. HARICA may include some informative data in the OU field to indicate certain human-readable information (for example text that a private key that corresponds to a certificate has been generated in a QSCD).

3.2.5 Validation of Authority

HARICA has implemented a procedure to determine the authorized individuals that can request certificates on behalf of an organization. Each organization may limit authorized certificate requestors. If an Applicant specifies, in writing, the individuals who may request a Certificate, then HARICA SHALL NOT accept any certificate requests that are outside this specification. HARICA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

Registration Authorities have procedures per which the Applicant's status and relationship with the institution are being verified. This is possible either with electronic lists assembled by each RA from the qualified - for each category- sources (e.g. secretariats of departments /faculties, institution's central registry etc.), or by presenting official certificates where the relationship of the Applicant with the institution is certified.

HARICA uses information from data sources per section 3.2.2.7 to establish a reliable method of communication.

For the issuance of EV Certificates, HARICA SHALL verify the Applicant's authorization, including:

- The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester, as per Section 3.2.8 of the EV Guidelines,
- That a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use, as per Section 3.2.9 of the EV Guidelines; and
- That a Certificate Approver has signed or otherwise approved the EV Certificate Request, as per Section 3.2.10 of the EV Guidelines.

3.2.6 Criteria for interoperability

HARICA may issue cross-certificates to assist ROOT roll-over operations. HARICA may also provide interoperation services to certify a non-HARICA CA. For such interoperation services to be provided, the following criteria must be met:

- The interoperation period will be limited to eight (8) years' maximum with a right to renew;
- A formal contract must be entered with HARICA, which includes a "right to audit" clause; and
- The CA must operate under a CP/CPS that is at least as strict as the HARICA CP/CPS.

Some Application Software Suppliers have specific procedures for approving cross-certification of a non-HARICA CA. In such cases, HARICA SHALL NOT issue a

cross-certificate to a non-affiliated entity without the expressed approval of those Application Software Suppliers.

HARICA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

3.3 Identification and Authentication for Re-key Requests

Re-keying (also known as "reissuing") refers to the creation of an entirely new certificate, using some or all information submitted for an existing certificate and using a newly generated Key Pair. Subscribers may request re-keying of a certificate only prior to the certificate's expiration. The re-keying process is described in section 4.7.

3.3.1 Identification and authentication for routine re-key

A Subscriber can request a routine re-key of an unexpired and unrevoked certificate, at any time before the expiration of the existing certificate, following the procedures described in section 3.2.

3.3.2 Identification and authentication for re-key after revocation

A Subscriber can request a routine re-key after a certificate revocation, following the described procedures in section 3.2.

3.4 Identification and authentication for revocation requests

In addition to the revocation cases described in sections 4.9.1.1 and 4.9.1.2, HARICA may revoke any certificate (Subordinate CA Certificate or end-entity Certificate) at its sole discretion.

Identification and authentication for revocation requests follow the methods described in section 3.2.3. Moreover, HARICA and the Subscriber may agree to a secret revocation code during the initial retrieval of the certificate, which may be used for the revocation of the certificate by the Subscriber.
Governmental regulatory authorities are authenticated via secure callback to their official telephone numbers or official email addresses.

The entire revocation process is described in section 4.9.3.

3.4.1 Revocation request from Issuing Authority

The Issuing CA shall revoke certificates if it has substantial evidence that a Subscriber's private key or a certificate is compromised. It may also revoke a certificate without Subscriber's consent if a certificate has been issued with incorrect parameters/information as described in section 4.9.1.1.

3.4.2 Revocation request from Subscriber

The Subscriber can request a certificate revocation to a secure HARICA interface, by using approved authentication methods or via a secret revocation code. Alternatively, a Subscriber may request a certificate revocation by making a call to the appropriate CA in which case an identity verification SHALL take place, using pre-existing information.

3.4.3 Revocation request from non-Subscriber

Certificate Revocation Requests from non-Subscribers requesting revocation of a HARICA Certificate, must follow the process described in section 4.9.3.2.

4 Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who is eligible to submit a certificate request

Certificate requests may be submitted by Applicants as described in section 1.3.3.

HARICA may utilize Google Safe Browsing engine to detect suspicious web sites and block Certificate issuance for associated Domain Names.

HARICA shall only issue QEVCP-w, QEVCP-w-psd2, EV SSL and EV Code Signing Certificates to Applicants which submit a complete Certificate Request and meet the requirements specified in sections 4.1.1 and 4.1.2 of the EV Guidelines, in addition to the requirements set in this CP/CPS.

4.1.2 Enrollment process and responsibilities

Prior to the issuance of a Certificate, HARICA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in section 4.2.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

The certificate request SHALL contain a statement from the Applicant or the Applicant Representative for the issuance of a Certificate, that all information contained therein is correct.

Applicants may submit a certificate application request through a secure web interface https://app.harica.gr/, https://cm.harica.gr, or through the registration office of her/his own institution, or Delegated Third Party RA, or through HARICA's central RA. The application process will result in the secure submission of a properly formatted CSR and identity verification evidence which will later be validated by Validation Specialists.

4.1.2.1 Enrollment process for EV Certificates

The following Applicant roles are required for the issuance of an EV Certificate:

1. **Certificate Requester:** The EV Certificate Request must be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

2. **Certificate Approver:** The EV Certificate Request must be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
3. **Contract Signer:** A Subscriber Agreement applicable to the requested EV Certificate must be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
4. **Applicant Representative:** In the case where HARICA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate must be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant may authorize one individual to occupy two or more of these roles, and/or may authorize more than one individual to occupy any of these roles.

4.2 Certificate Application Processing

4.2.1 Subscriber identification and authentication procedures

The processing of the certificate applications is outlined in section 3.2. All certificate applications are checked for validity. The Applicant SHALL verify all data requested for inclusion in a Certificate.

In cases where the certificate request does not contain all the necessary information about the Applicant, HARICA SHALL obtain the remaining information from the Applicant or, having obtained it from a Reliable Data Source, confirm it with the Applicant.

Section 6.3.2 limits the validity period of Subscriber Certificates. HARICA MAY use the documents and data provided in section 3.2 to verify certificate information, or may reuse previous validations themselves, including validation of authority, provided that HARICA obtained the data or document from a source specified under section 3.2 or completed the validation itself.

The maximum Subject Identity Information reuse period of Certificates shall be:

- for Qualified Certificates for Electronic Signatures or Electronic Seals or Website Authentication, **three hundred sixty-five (365) days**;
- for SSL/TLS Client Authentication, OV Code Signing, S/MIME and non-Qualified Document Signing Certificates, **eight hundred twenty-five (825) days**;
- for SSL/TLS Server Authentication Certificates:
  - **eight hundred twenty-five (825) days** until March 15, 2026,
  - **Effective** 2026-03-15, **three hundred ninety-eight (398) days**.

The maximum Domain Name and IP Addresses reuse period of SSL/TLS Server Authentication Certificates shall be:

- **three hundred ninety-eight (398) days** until March 15, 2026,
- **effective** 2026-03-15, **two hundred (200) days**,
- **effective** 2027-03-15, **one hundred (100) days**,
- **effective** 2029-03-15, **ten (10) days**.

For EV Certificates, except for reissuance of an EV Certificate under section 3.2.14.2 of the EV Guidelines and except when permitted otherwise in section 3.2.14.1 of the EV Guidelines, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

(A) Legal existence and identity – **three hundred ninety-eight (398) days**;
(B) Assumed name – **three hundred ninety-eight (398) days**;
(C) Address of Place of Business – **three hundred ninety-eight (398) days**;
(D) Verified Method of Communication – **three hundred ninety-eight (398) days** ;
(E) Operational existence – **three hundred ninety-eight (398) days**;
(F) Domain Name – **three hundred ninety-eight (398) days**;
(G) Name, Title, Agency, and Authority – **three hundred ninety-eight (398) days**, unless a contract between HARICA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or HARICA, or until the contract expires or is terminated.

The three hundred ninety-eight (398) days period set forth above SHALL begin to run on the date the information was collected by HARICA.

HARICA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under sections 3.2.9 and 3.2.10 of the EV Guidelines.

HARICA MAY reuse Subscriber Private Key protection validations of methods 4, 5 and 7 of section 6.2.7.4.2 no more than thirteen (13) months prior to issuing a Code Signing Certificate.

HARICA SHALL repeat the verification process for any information obtained outside the time limits specified above except when permitted otherwise under section 3.2.14.1 of the EV Guidelines.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

4.2.2 Approval or rejection of certificate applications

After all identity and attribute checks of the Applicant take place, the content of the application for the Certificate is also checked. In case the Applicant is not eligible for a Certificate or the application contains errors, the application is rejected.

HARICA shall reject requests for Certificates where all required validation steps cannot be successfully completed.

HARICA SHALL NOT issue Certificates containing Internal Names, Reserved IP addresses and Certificates containing Domain Names that end in an IP Reverse Zone Suffix.

HARICA may reject a request for any Certificate the issuance of which may harm, diminish or otherwise negatively impact HARICA, including Relying Parties. HARICA shall be the sole determinant of what meets the criteria in the previous paragraph, without being obligated to provide a reason for rejection of any Certificate Request.

HARICA SHALL NOT issue new or replacement Code Signing Certificates to an entity that HARICA determined intentionally signed Suspect Code. HARICA shall keep meta-data about the reason for revoking a Code Signing Certificate as proof that the Code Signing Certificate was revoked because the Applicant was intentionally signing Suspect Code.

HARICA MAY issue new or replacement Code Signing Certificates to an entity who is the victim of a documented Takeover Attack, resulting in a loss of control of the Private Key associated with their Code Signing Certificate. Documentation of a Takeover Attack MAY include a police report (validated by HARICA) or public news report that admits that the attack took place. The Subscriber MUST provide a report from an auditor with IT and security training or a CISA that provides information on how the Subscriber was storing and using Private Keys and how the intended solution for better security meets the guidelines for improved security.

Successfully verified and validated certificate applications which meet the criteria for the requested certificate, shall be approved.

Subscribers requesting or utilizing Code Signing Certificates must observe the requirements for Private Key generation and protection provided in section 6.2.7.4.

EV Certificate requests shall require a minimum of two (2) separate Validation Specialists for approval. The second Validation Specialist requires additional documentation and/or verification before approving the issuance an EV certificate. In no case shall an EV Certificate be validated, authorized or issued by one individual. See also section 5.2.4.

4.2.3 Time to process certificate applications

The certificate applications are processed within a period of **ten (10)** business days maximum, apart from the cases of force majeure.

4.2.4 Certificate Authority Authorization (CAA)

HARICA shall review CAA records as defined in RFC 6844 before issuing Subscriber Certificates used for SSL/TLS or Subordinate CA Certificates capable of issuing Subscriber Certificates for SSL/TLS, except for optional cases described in section 3.2.2.8.

HARICA does not currently process CAA records for Mailbox Addresses.

Subscribers who wish to authorize HARICA to issue server TLS Certificates for their FQDNs should include in their respective DNS zone a CAA record property `issue` or `issuewild`, including the value "**harica.gr**".
Subscribers who wish to authorize HARICA to issue S/MIME Certificates for their Mailbox Addresses should include in their respective DNS zone a CAA record property `issuemail`, including the value "**harica.gr**".

Starting on **March 15, 2025** prior to issuing a Certificate that includes a Mailbox Address HARICA SHALL retrieve and process CAA records in accordance with Section 4 of RFC 9495.

When processing CAA records, HARICA SHALL process the `issuemail` property tag as specified in RFC 9495. Additional property tags MAY be supported, but SHALL NOT conflict with or supersede the authorizations to issue S/MIME Certificates as specified in the `issuemail` property tag.

If HARICA issues a Certificate following a CAA check, it SHALL do so within the TTL of the CAA record, or 8 hours, whichever is greater. This stipulation does not prevent HARICA from checking CAA records at any other time.

If the Certificate includes more than one Mailbox Address, then HARICA SHALL perform the above procedure for each Mailbox Address.

CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Technically Constrained Subordinate CA Applicant.

HARICA SHALL NOT issue a Certificate unless HARICA determines that Certificate Request is consistent with the applicable CAA RRset. HARICA SHALL log all actions taken, if any, consistent with its CAA processing practice.

Subscribers who already have CAA entries in their respective DNS zone and need a server TLS or S/MIME Certificate from HARICA SHALL add a CAA record property `issue`/`issuewild` or `issuemail` respectively, with the value "**harica.gr**".

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate issuance

Subscriber certificates are published after the successful verification of the contents of the Certificate by the Subscriber.

Certificate issuance by a Root CA shall require an individual authorized by HARICA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command for the Root CA to perform a certificate signing operation.

HARICA discloses all CA Certificates to its official repository. CA certificates chaining to a CA Certificate included in Application Software Supplier's Root Stores that are members of the CCADB, SHALL be disclosed to the CCADB within seven (7) calendar days of issuance and before the CA Certificate is used to issue Publicly-Trusted Certificates.

Pre-issuance linting checks shall take place to verify compliance with applicable standards according to each certificate type.

For SSL/TLS Certificates that need to be trusted by Application Software Suppliers, HARICA shall log the precertificates in at least two Certificate Transparency log servers. These log servers must be qualified and trusted by such Application Software Suppliers.

4.3.2 Notification to Subscribers by the CA regarding issuance of certificate

HARICA informs the Applicant about the acceptance or rejection of the Certificate Application, via email.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

During the application process, the Subscriber has reviewed and verified the information to be included in the Certificate.

Failure of the Subscriber to object to the Certificate or its content within 24 hours from downloading it constitutes Certificate acceptance.

4.4.2 Publication of the certificate by the CA

All CAs publish the certificates only after the Applicants have retrieved them per section 4.4.1.

4.4.3 Notification of other entities about certificate issuance by the CA

No action is taken for the notification of other entities other than what is stated in section 4.3.1.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Subscribers can use their private keys and certificates for the usages stated in section 6.1.7. They must also follow the Subscriber Warranties as described in section 9.6.3, especially the ones related to the "Protection of Private Key" and "Use of Certificate".

4.5.2 Relying party public key and certificate usage

Relying parties can use the Subscribers' public keys and certificates after following the requirements of section 1.3.4. The operations they can execute (this list is not limited) are:

- Verification of digitally signed email messages using the S/MIME protocol
- Encryption of email messages using the S/MIME protocol
- Verification of digitally signed documents/application code
- Verification of digital timestamps in documents
- Encryption of files, data and communication channels
- Authentication
- Authorization

4.6 Certificate Renewal

4.6.1 Prerequisite Circumstances for certificate renewal

A Certificate renewal is permitted when an un-revoked certificate is almost expired. Some certificates may be renewed using the same key pair if the key lifetime of the certificates is not exceeded. Furthermore, everything listed in section 1.3.3 applies. The lifetimes are stated in section 6.3.2. It is recommended that all certificates are renewed using new key-pairs.

4.6.2 Who may request renewal

The Subscriber wishing renewal through a HARICA secure endpoint, submits the renewal request after proper authentication. It is recommended that Subscribers receive a notification message from the Registration Authority **fifteen (15) days** before the expiry date of their certificate and are informed for its imminent expiry.

4.6.3 Processing certificate renewal requests

- Initially, a check whether renewals of the same certificate were made in the past takes place.
- Afterwards a check whether the certificate or the certificates containing the same key exist for a smaller duration than the maximum validity period and that the key satisfies current cryptographic security standards takes place.
- Additionally, if any Subject attributes, such as the certified common name or email address, have changed, the procedures for a new certificate application take place.
- For the rest of the permitted key validity period a new certificate is issued using the original CSR.

For instance, a Subscriber who has an existing certificate with a one-year validity period can renew it (without changing the private key) for another year, since the maximum validity period of the private key is more than one year (according to section 6.3.2). If

a Subscriber Certificate is revoked due to a `keyCompromise` reason, the Public Key associated with that Certificate cannot be re-used in a new Certificate Request.

4.6.4 Notification of new certificate issuance to Subscriber

As stated in section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

As stated in section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

As stated in section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

As stated in section 4.4.3.

4.7 Certificate Re-keying

4.7.1 Circumstance for certificate re-keying

Certificate re-keying is the re-issuance of a certificate using the same subject information and expiration date ("validTo" field) but with a new key-pair. Furthermore, everything listed in section 1.3.3 applies. Reasons for re-keying may be (this list is not restrictive):

- The discovery of a vulnerability in a key algorithm or key size
- The loss or compromise or suspicion of compromise of a private key
- The deprecation of a key algorithm or key size

4.7.2 Who may request certification of a new public key

Subscribers may re-key a certificate via a secure endpoint after proper authentication. The previously used certificate is usually revoked.

4.7.3 Processing certificate re-keying requests

As described in section 4.3.

4.7.4 Notification of new re-keyed certificate issuance to Subscriber

As described in section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As described in section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

As stated in section 4.4.2.

4.7.7 Notification of re-keyed certificate issuance by the CA to other entities

As stated in section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

Modification of end-entity certificate subject details is not permitted. In case there is a mistake during certificate issuance (e.g. spelling), the certificate is revoked and the issuance process is followed, as stated in section 4.3.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to Subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of the certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate Revocation and Suspension

This section applies to CA and end-entity Certificates. It does not apply to Short-term Certificates for eSignatures or eSeals which cannot be revoked.

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

With the exception of Short-term Certificates, a Certificate must be revoked when the subject fields it contains have changed or when the corresponding Private Key has been proven to be compromised. In the latter case, if anyone that requests revocation has previously demonstrated or can currently demonstrate possession of the Private Key of the Certificate, all Certificates that include the Public Key corresponding to the compromised Private Key must be revoked by HARICA and that Public Key cannot be re-used in a Certificate Signing Request. Otherwise, if the Subscriber has not previously demonstrated and cannot currently demonstrate possession of the associated Private Key of that certificate, HARICA may revoke all Certificates that include the Public Key corresponding to the compromised Private Key or block issuance of future Certificates with that key.

Moreover, the certificate may be revoked when the Applicant has not accepted it in the time interval defined in section 4.4.1 or if it has been proven that the usage of the

certificate does not conform to this CP/CPS. Finally, it must be revoked if it contains erroneous information.

4.9.1.1.1 Revocation Reasons based on ITU-T X.509 and RFC 5280

With the exception of Short-term Certificates, HARICA SHALL revoke any Subscriber Certificate within twenty-four (24) hours and use the corresponding CRLReason (see section 7.2.2) if one or more of the following occurs (please note that a *keyCompromise* CRLReason takes precedence over other revocation reasons):

1. The Subscriber requests in writing, without specifying a CRLreason, that HARICA revoke the Certificate for a reason not listed below (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL) ;
2. The Subscriber notifies HARICA that the original Certificate Request was not authorized and does not retroactively grant authorization. This also applies for Qualified Certificates for electronic seals where there is a change in Legal representation and the former Legal representative is no longer authorized to create Electronic Seals (CRLReason #9, privilegeWithdrawn);
3. HARICA obtains verifiable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. HARICA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address or mailbox control for any Mailbox Address in the Certificate should not be relied upon (CRLReason #4, superseded);
5. HARICA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise (CRLReason #1, keyCompromise);
6. There is clear evidence that the specific method used to generate the private key was flawed (CRLReason #1, keyCompromise);
7. HARICA 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 Section 6.1.1.3(5) (CRLReason #1, keyCompromise);

With the exception of Short-term Certificates, HARICA SHOULD revoke any Subscriber Certificate within twenty-four (24) hours and SHALL revoke a Certificate within five (5) days if one or more of the following occurs:

8. HARICA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
9. HARICA is made aware that the Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
10. HARICA is made aware that a wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified domain name (CRLReason #9, privilegeWithdrawn);
11. HARICA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);

12. HARICA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
13. The Subscriber no longer controls, or is no longer authorized to use, all of the Domain Names or email addresses in the Certificate (CRLReason #5, cessationOfOperation);
14. The Subscriber will no longer be using the Certificate because they are discontinuing their website or email address (CRLReason #5, cessationOfOperation);
15. HARICA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or an email address in the Certificate is no longer legally permitted. This could be a result of a court or arbitrator revoking a Domain Name Registrant's right to use an email address or a 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. The same applies if a natural person, whose information is included in the Subject field of the Certificate, is no longer associated with an organization included in the "Organization" field of the Certificate (CRLReason #5, cessationOfOperation);
16. HARICA has replaced the Certificate due to changes in the Certificate's subject information and no other reason is applicable (CRLReason #3, affiliationChanged);
17. The Subscriber has requested a new Certificate to replace an existing Certificate and no other reason is applicable (CRLReason #4, superseded);
18. HARICA has revoked the Certificate for compliance reasons such as the Certificate does not comply with this policy, the CA/Browser Forum's Baseline Requirements, or HARICA's CP/CPS (CRLReason #4, superseded);
19. HARICA's right to issue Certificates under this CP/CPS expires or is revoked or terminated, unless HARICA has planned to continue maintaining the CRL/OCSP Repository (unspecified);
20. For Code Signing Certificates: The Application Software Supplier requests revocation (unspecified);
21. For Code Signing Certificates: If a third party provides information that the Certificate has been used to sign Suspect Code, HARICA shall investigate the request and revoke the Code Signing Certificate in accordance with section 4.9.4 (unspecified).

In addition to the reasons mentioned above, with the exception of Short-term Certificates, HARICA shall revoke a Qualified Certificate if any of the following event occurs:

22. The National Supervisory Body, during its surveillance duties, rules that a Qualified Certificate contains false or inaccurate information, not-conformant to the eIDAS Regulation (CRLReason #4, superseded);
23. HARICA declares termination of services with no successor solution (unspecified);
24. HARICA becomes aware that the Subscriber no longer has the signing right, is declared non-existent, is deceased, considering that Qualified Certificates for electronic signatures are in all cases non-transferable (CRLReason #5, cessationOfOperation);

25. HARICA receives a court order with a final ruling that orders HARICA to revoke a Qualified Certificate (CRLReason #5, cessationOfOperation);

Especially for PSD2 Certificates, HARICA shall follow the provisions of clause 6.2.6 of ETSI TS 119 495 and revoke such Certificate if requested by the National Competent Authority (NCA), as the owner of the PSD2 specific information, if:

26. The authorization of the PSP has been revoked (CRLReason #5, cessationOfOperation);
27. Any PSP role included in the Certificate has been revoked (CRLReason #5, cessationOfOperation).

Finally, except for "privilegeWithdrawn", the Subscriber will have the option to select one of the above reasons that best matches their circumstances to revoke a TLS certificate. When none of the reasons apply to the revocation request, the subscriber should not provide a reason other than "unspecified" (default value).

For Code Signing Certificates HARICA MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

HARICA shall revoke a Subordinate CA Certificate technically capable of issuing TLS and Code Signing Certificates within seven (7) days if one or more of the following occurs:

1. An Externally Operated Subordinate CA, requests revocation in writing;
2. An Externally Operated Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Private Key corresponding to the Public Key in the Subordinate CA Certificate suffered a Key Compromise or no longer complies with the requirements of sections 6.1.5 and 6.1.6,
4. The Issuing CA obtains evidence that the Private Key corresponding to the Public Key in the Subordinate CA Certificate was misused;
5. The Issuing CA is made aware that the Subordinate CA Certificate was not issued in accordance with, or that the Externally Operated Subordinate CA has not complied with the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not planned for another CA to provide revocation support for the Subordinate CA Certificate;

8. The Issuing CA's or Subordinate CA's right to issue Certificates under this CP/CPS expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

HARICA shall revoke a Subordinate CA Certificate technically capable of issuing client authentication, S/MIME, eSignature and eSeal Certificates if one or more of the reasons above occurs.

4.9.2 Who can request a revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties including governmental regulatory authorities and courts per the local and European legislation, may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

4.9.3.1 Certificate revocation by the Subscriber

The validation of the Subscriber's identity is required per section 3.4. After revocation, the Subscriber will be informed of the change of status and the certificate shall never be reinstated.

4.9.3.2 Certificate revocation by any other entity

Any other entity can submit a Certificate Problem Report that might also include a revocation request via email as described in section 1.5.2 with proof that:

a) the private key of the certificate has been exposed, or
b) the use of the certificate does not conform to the Certificate Policy or
c) the certificate owner's relationship with the corresponding organization is terminated.

All third-party revocation requests are investigated by HARICA before a revocation action is taken.

After revocation, the Subscriber of the certificate will be informed of the change of status and the certificate shall not be reinstated.
For submitting a high-priority Certificate Problem Report, use the contact information provided in section 1.5.2.

4.9.3.3 Revocation request by an Application Software Supplier

If an Application Software Supplier believes that a Certificate attribute is deceptive, or that the Certificate is being used to sign Suspect Code, or some other illicit purpose, then the Application Software Supplier may request that HARICA revoke the certificate to a specific date.

In such a case, within two (2) business days of receipt of the request, HARICA SHALL either revoke the certificate or inform the Application Software Supplier that it is

conducting an investigation. If HARICA decides to conduct an investigation, it SHALL inform the Application Software Supplier whether or not it will revoke the Certificate, within two (2) business days. If HARICA decides that the revocation will have an unreasonable impact on the Subscriber, then HARICA SHALL propose an alternative course of action to the Application Software Supplier based on its investigation.

In all cases, the Subscriber shall be notified prior to any status change of their Certificate.

4.9.3.4 Revocation request by the eIDAS National Supervisory Body

If the National Supervisory Body (EETT) believes that a Qualified Certificate includes information that is incorrect or misleading, or that the Certificate is Compromised or being used to sign falsified data, or some other illicit purpose, then the Supervisory Body may request that HARICA suspends or revokes the Qualified Certificate. The Supervisory Body must specify a revocation reason based on Article 11 of the Trust Service Providers National regulation (FEK 4396-B, 2017).

In such a case, HARICA must authenticate the revocation request and execute the request within two (2) business days. In all cases, the Subscriber shall be notified prior to any status change of their Certificate.

4.9.3.5 Revocation request by a National Competent Authority

If a PSD2 National Competent Authority (NCA) believes that a PSD2 Qualified Certificate includes information for a PSP that is incorrect or misleading, or that the Certificate is Compromised or being used to sign falsified data, or some other illicit purpose, then the NCA may request that HARICA suspends or revokes the PSD2 Qualified Certificate. The NCA must specify a revocation reason, which must be descriptive rather than in a standard form. Valid reasons for revocation can include the following scenarios:

- information in the Public Register has changed to substantially affect the validity of the PSD2 attributes in the certificate;
- the authorization status granted by that NCA has changed (e.g. that PSP is no longer authorized).

In such a case, HARICA must authenticate the revocation request and execute the request within two (2) business days. In all cases, the Subscriber shall be notified prior to any status change of their Certificate.

4.9.4 Revocation request grace period

The Subscriber can make a revocation request anytime during the validity period of the certificate.

For all incidents involving Key Compromise of Certificates used for Code Signing, e-Signatures or e-Seals, HARICA SHALL revoke the Signing Certificate in accordance with and within the following maximum timeframes. Nothing herein prohibits HARICA from revoking a Code Signing Certificate prior to these timeframes.

1. HARICA SHALL contact the Subscriber within one (1) business day after HARICA is made aware of the incident.
2. HARICA SHALL determine the volume of relying parties that are impacted (e.g., based on OCSP logs) within 72 hours after being made aware of the incident.
3. HARICA SHALL request the Subscriber to send an acknowledgement to HARICA within 72 hours of receipt of the request.

   a. If the Subscriber responds within 72 hours, HARICA and the Subscriber SHALL determine a "reasonable date" to revoke the Certificate based on discussions with HARICA.
   b. If the Subscriber does NOT respond within 72 hours, HARICA SHALL notify the Subscriber that HARICA will revoke the Certificate in 7 days if no further response is received.
      i. If the Subscriber responds within 7 days, HARICA and the Subscriber will determine a "reasonable date" to revoke the Certificate based on discussions with HARICA.
      ii. If the Subscriber does NOT respond after 7 days, HARICA SHALL revoke the Certificate, except if HARICA has documented proof (e.g., OCSP logs) that this will cause significant negative impact to the general public.

4.9.4.1 Revocation dates for “Signature” Certificates

When revoking a Subscriber Certificate used for Code Signing, e-Signatures or e-Seals, due to a Key Compromise or use in Suspect Code HARICA SHALL determine an appropriate value for the revocationDate based on its own investigation. HARICA SHALL set a historic date as `revocationDate` if deemed appropriate. This `revocationDate` should be used as the revocation timestamp for Code Signing Certificates to block the execution of Suspect Code. The same applies to Certificates for e-Signatures or e-Seals, to invalidate e-Signatures and e-Seals of signed documents after the suspected compromise. This is called a back-dated revocation and applies only to Certificates used for “Signing” objects.

4.9.5 Time within which CA must process the revocation request

Within twenty-four (24) hours, except from force majeure cases, after receiving a Certificate Problem Report, HARICA SHALL investigate the facts and circumstances related to a 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, HARICA SHALL 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 HARICA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation SHALL NOT exceed the time frame set forth in section 4.9.1.1. The date selected by HARICA SHOULD 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.

Revocation requests that provide adequate supporting evidence will be processed immediately. The maximum delay between the confirmation of the revocation of a certificate to become effective and the actual change of the status information of this certificate being made available to relying parties, shall be at most **sixty (60)** minutes.

4.9.6 Revocation checking requirement for relying parties

Relying parties must follow the procedures described in section 1.3.4 before they rely on any certificate. They should load the Certificate Revocation Lists of all the Subordinate CA Certificates that chain to a trust anchor. The Revocation lists are always published in the Repository and are publicly available via a publicly-accessible HTTP URL. A Certificate Revocation List shall include the status of a certificate at least until its expiration. If OCSP URL is available via the `authorityInformationAccess` extension, and the OCSP responder is available within the operational limits described in section 4.10.1, Relying Parties must check the revocation status of all Certificates (including the status of Subordinate CA Certificates) via OCSP.

4.9.7 CRL issuance frequency

CRLs shall be signed by the corresponding Issuing CA and shall be stored in a protected environment to ensure their integrity and authenticity.

Within twenty-four (24) hours of issuing its first Certificate, the CA MUST generate and publish either:

- a full and complete CRL; OR
- partitioned (i.e., "sharded") CRLs that, when aggregated, represent the equivalent of a full and complete CRL.

CAs issuing Subscriber Certificates:

1. MUST 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 responder location”); or
    - **four (4) days** in all other cases;
2. MUST update and publish a new CRL **within twenty-four (24) hours** after recording a Certificate as revoked.

CAs issuing CA Certificates and end-entity Certificates that contain an EKU which includes id-kp-timeStamping (as defined in RFC 5280):

1. MUST update and publish a new CRL at least **every twelve (12) months**;
2. MUST update and publish a new CRL **within twenty-four (24) hours** after recording a Certificate as revoked.

CAs MUST continue issuing CRLs until one of the following is true:

- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR
- the corresponding Subordinate CA Private Key is destroyed.

In case of secret key exposure or of any other important security compromise incident, for example a Subordinate CA Certificate or a Time-Stamping Unit Certificate revocation, an updated Certificate Revocation List SHALL be published within **twenty-four (24) hours** from the revocation timestamp.

4.9.8 Maximum latency for CRLs

After a certificate revocation, the CRL is issued and the repository is updated. The CRL is published at the Repository within minutes of its issuance. The certificate is marked as revoked in the Repository.

HARICA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

4.9.9 Online revocation/status checking availability (OCSP)

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, associated with the Issuing CA.

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

The following SHALL apply for communicating the status of Certificates which include an Authority Information Access extension with an `id-ad-ocsp` accessMethod.
OCSP responses SHALL conform to RFC 6960 and/or RFC 5019. HARICA MAY process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954

OCSP responses SHALL either:

1. Be signed by the Issuing CA whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the Issuing CA whose revocation status is being checked.

In the latter case, the OCSP signing Certificate SHALL contain an extension of type `id-pkix-ocsp-nocheck`, as defined by RFC 6960.

4.9.10 Online revocation checking requirements

HARICA supports OCSP capability using the GET method as described in RFC 6960.

For the status of a Subscriber Certificate or its corresponding Precertificate:

- an authoritative OCSP response SHALL be available (i.e. the responder SHALL NOT respond with the "unknown" status) starting no more than **fifteen (15) minutes** after the Certificate or Precertificate is first published or otherwise made available;
- For OCSP responses with validity intervals less than sixteen (16) hours, HARICA SHALL provide an updated OCSP response prior to **one-half** of the validity period before the `nextUpdate`.
- For OCSP responses with validity intervals greater than or equal to sixteen (16) hours, HARICA SHALL provide an updated OCSP response at least **eight (8) hours** prior to the `nextUpdate`, and no later than **four (4) days** after the `thisUpdate`.
- OCSP responses SHALL have a validity interval greater than or equal to **eight (8) hours** and less than or equal to **ten (10) days.**

For the status of Subordinate CA Certificates:

- HARICA SHALL provide an updated OCSP response at least (i) every **twelve (12) months** and (ii) within **twenty-four (24) hours** after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a certificate serial number that is "unassigned", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with section 7.1.5, the responder SHALL NOT respond with a "good" status for such requests.

4.9.11 Other forms of revocation advertisements available

The revoked certificates appear as “Revoked” in the search engine of the Certificate Repository.

If HARICA revokes a Subordinate CA Certificate that is already disclosed to the CCADB, it SHALL update the CCADB to mark that CA Certificate as revoked, including the reason for revocation, within seven (7) calendar days of revocation.

HARICA shall disclose a full CRL URL for each disclosed non-expired, non-revoked CA Certificate to the CCADB.

4.9.12 Special requirements regarding key compromise

As defined in section 4.9.1.

Non-Subscriber entities may report a Key Compromise of an unexpired, unrevoked HARICA Certificate according to the contact information described in section 4.9.3.2, using one of the following documented methods to prove possession/control of the private key associated with a Certificate. HARICA MAY allow additional, alternative methods that do not appear in this section at its own discretion.

4.9.12.1 Create and sign a test file

Create a text file with the content “This key is compromised” or similar language to indicate that the signer of this message claims this key is compromised. Use the following command from a command line terminal:

- `echo “This key is compromised” > compromised.txt`

Sign a sha256 hash of the produced file using the private key (in PEM format) you want to report as compromised, using openssl:

- `openssl dgst -sha256 -sign private-key.pem -out compromised.txt.signed compromised.txt`

Send the file “compromised.txt.signed” to HARICA according to section 4.9.3.2.

4.9.12.2 Create a CSR which includes a custom text

Create a CSR that includes in the `subject:commonName` field the text “This key is compromised” or similar language to indicate that the signer of this message claims this key is compromised. Use the following command from a command line terminal using openssl:

- `openssl req -new -key private-key.pem -subj "/CN=This key is compromised" -out compromised.csr`

Send the file “compromised.csr” to HARICA according to section 4.9.3.2.

4.9.12.3 Disclose the actual Private Key

This method is not recommended but will be considered proof of Key Compromise by HARICA.

Send the actual compromised private key to HARICA according to section 4.9.3.2.

4.9.13 Circumstances for suspension

Certificate suspension is not permitted for Certificates used for SSL/TLS or Code Signing. When HARICA receives a revocation request per sections 4.9.3.2 or 4.9.3.3, and depending on the findings during investigation, the suspension of Certificates is an option at HARICA’s sole discretion.

4.9.14 Who can request suspension

Certificate suspension may be requested by Relying Parties or Application Software Suppliers as described in sections 4.9.3.2 or 4.9.3.3 respectively.

4.9.15 Procedure for suspension request

Certificate suspension may be requested via the revocation request. The suspension of Certificates remains at HARICA's sole discretion. The affected Subscriber is always notified by HARICA for any Certificate status change, including Certificate suspension.

If HARICA decides to suspend a Certificate, the affected CRL is updated with a revoked certificate entry and revocation reason "`certificateHold`", per RFC 5280. If this Certificate is reinstated, the affected entry is removed. If the Certificate is revoked, this entry is updated and the revocation reason is modified accordingly. Once a Certificate is revoked, it cannot be reinstated.

4.9.16 Limits on suspension period

Certificate suspension cannot exceed two (2) weeks.

4.10 Certificate status services

4.10.1 Operational characteristics

HARICA SHALL provide accurate and up-to-date revocation status information for Certificates used for "authentication" (i.e. SSL/TLS) until these certificates expire.

HARICA SHALL provide accurate and up-to-date revocation status information for a period not less than **seven (7)** years beyond expiry of Certificates used for e-Signatures, e-Seals, Code Signing and Timestamp. After the expiration of an Issuing CA that issues Certificate used for e-Signatures, e-Seals, Code Signing and Timestamp, the associated CRLs shall remain published for at least **five (5)** years beyond the expiry of that Issuing CA. Application Software Suppliers MAY request HARICA to support a longer lifetime according to their trust store requirements.

HARICA SHALL provide OCSP Responses for e-Signature, e-Seal, Code Signing and Timestamp Certificates that include an AIA extension which contains the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1) until at least the expiration of the issuing CA Certificate.

Note: If a Code Signing Certificate contains the Lifetime Signing OID, the digital signature becomes invalid when the Code Signing Certificate expires, even if the digital signature is timestamped.

HARICA shall include URLs to revocation information (where applicable) within any end-entity Certificate in CRL Distribution Points and Authority Information Access extensions.

4.10.1.1 Online Certificate status service OCSP

As defined in section 4.9.10.

4.10.1.2 Online Certificate Repository

No stipulation.

4.10.1.3 Usage of Certificate Revocation Lists (CRL)

As defined in section 4.9.6.

4.10.2 Service Availability

HARICA performs all the necessary actions for the uninterruptible - as possible - availability of its OCSP service.

HARICA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

4.10.3 Optional features

If a CA supports multiple methods (CRL and OCSP service) to provide revocation status, the information provided by all services shall be consistent over time, taking into account different delays in updating the status information for all the methods. Consistency over time allows for the difference in delays to be taken into account provided that the status of the certificate is ultimately the same.

For example, if OCSP responses can be updated immediately, OCSP and CRL may differ, until the new CRL has been generated.

In case of inconsistency between the OCSP and CRL status of a certificate, the "Revoked" status from either status service shall take precedence by Relying Parties.

4.11 End of subscription

The subscription is terminated when a Certificate

- reaches the "`validTo`" date and expires
- is revoked before reaching the "`validTo`" date.

Revocation of an expired certificate is not necessary unless there is a reason such as the ones referred in section 4.9.1.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

HARICA does not currently support subscriber key escrow.

4.12.2 Session key encapsulation and recovery policy and practices

HARICA does not currently support subscriber key escrow.

5 Administrative, Technical and Operational Controls

5.1 Physical security and access controls

5.1.1 Site location

HARICA is currently operated by the IT Center of Aristotle University of Thessaloniki. CA/RA equipment is in secure and geographically diverse data centers.

Equipment, information and software relating to the Certification Authority and Registration Authority functions are constantly monitored and shall not be taken off-site without prior authorization by the senior management of HARICA.

5.1.2 Physical access

Physical access to the equipment of the CAs and the RAs is only allowed to authorized personnel in trusted roles.

HARICA CA equipment are in locked cabinets in locked server rooms. Access to the server rooms is monitored and always controlled.

In case unauthorized personnel need to enter the physical location of the CAs and the RAs, they must be under constant supervision by an authorized person.

5.1.3 Power and cooling

All CA equipment is in air-conditioned rooms with power supply protected by Uninterruptible Power Supply units (UPS) and backup power generators.

5.1.4 Water exposures

CA equipment is located on raised flooring and not largely exposed to water.

5.1.5 Fire prevention and protection

CA equipment is subject to the Greek law on prevention and fire protection in public buildings.

5.1.6 Media storage

HARICA private keys associated with CA Certificates are stored in secure external storage media in encrypted form and distributed only to authorized personnel, requiring at least two trusted individuals to access the keys. No single member of the authorized personnel has the capability to access a backup key.

Backups of HARICA CA/RA software, RA archive and audit logs are stored in removable media in encrypted form.

Both previously mentioned storage media are in distant physical locations, protected from exposure to water and fire. Appropriate measures have been taken to protect all media from deterioration.

If reusable media storage is used (e.g. memory flash disks) files shall be securely deleted to avoid object re-use, using methods described in section 6.2.10.

In case media storage is encrypted, the destruction of the decryption key is sufficient to consider that the encrypted media is destroyed.

5.1.7 Waste Disposal

Waste containing any confidential information, such as floppy disks, hard disks etc. are destroyed before being discarded. TSU private signing keys stored on TSU cryptographic module shall be erased upon device retirement in a way that it is practically impossible to recover them.

5.1.8 Off-site backup

There are off-site backups of software and data used in the HARICA PKI. Backups of HARICA CA/RA software, RA archive and audit logs are stored in removable media in encrypted form, accessible to authorized personnel. CA private keys are also stored off-site in encrypted form, accessible only by authorized personnel, following stipulations from section 5.2.2.

5.2 Procedural controls

5.2.1 Trusted roles

Personnel assigned to operate the HARICA PKI occupy a documented and well-defined trusted role. Each trusted role is authorized to perform specific tasks related to the Certification and Registration Authorities operations under well-defined procedures. The trusted roles and job descriptions of all personnel are clearly identified. Based on the trusted roles, a separation of duties takes place, and the least privilege principle applies in the user account management and access control procedures.

Personnel assigned to administer the servers of the Registration Authorities are also authorized to back up the transaction log files.

5.2.2 Number of persons required per task

PKI-sensitive operations require active participation of at least two authorized individuals to perform the sensitive operation. CA private keys are backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3 Identification and authentication for each role

A person holding a trusted role must authenticate to the Certificate Management System or the RA Management System before performing any duties, using a unique credential created by or assigned to that person.

5.2.4 Roles requiring separation of duties

Personnel assigned the Internal Auditor trusted role, shall not occupy another trusted role when performing CA key ceremony procedures.
For EV Certificates, HARICA enforces the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV

Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in section 3.2.13 of the EV Guidelines, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Certificate.

5.3 Personnel controls

5.3.1 Qualifications, experience and clearance requirements

Personnel handling roles of Certification Authorities and Registration Authorities must have experience in digital certificates and the Public Key Infrastructure domain. They must also have experience in managing sensitive personal data and classified information in general. Enough personnel possessing the expert knowledge shall be employed or contracted.

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor, HARICA verifies the identity and trustworthiness of such person.

5.3.2 Background check procedures

Personnel handling Certification Authorities and Registration Authorities comply with the applicable laws and framework.

All personnel shall be free from all conflicting interests.

5.3.3 Training requirements

Personnel with access to cryptographic procedures, is trained and educated on CA/RA operations by HARICA PKI experts. For this purpose, there is adequate documentation that describes all the operational procedures of the infrastructure. Personnel working for HARICA need to be familiar and understand all relevant policies, procedures and this CP/CPS. Validation Specialists are trained and tested to the EV Certificate validation criteria.

5.3.4 Re-training frequency and requirements

Personnel operating in trusted roles maintain high skill level. Whenever there are new developments in the PKI industry/technology or operational changes, a training seminar is scheduled, and the proper information is disseminated to the staff.

HARICA informs Validation Specialists and personnel operating Certificate Management Systems about security-related incidents of other TSPs issuing Publicly Trusted Certificates, and any related discussions/challenges/best practices identified in standards organizations such as the CA/Browser Forum, ETSI and ENISA.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

All legal procedures prescribed for certain offenses are followed, including disciplinary actions according to HARICA’s Security Policy and internal procedures.

5.3.7 Independent contractor's requirements working outside GUnet and involved with the HARICA PKI

In case HARICA hires an independent contractor for audit or other operations, the contractor is obliged to sign a Non-Disclosure Agreement contract. The same principle applies for external auditors.

HARICA SHALL verify that a Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Sections 5.4.1 and 5.5.1.

5.3.8 Documentation supplied to the personnel

Relevant documentation is available to trainees who undertake specific roles within the HARICA PKI.

5.4 Audit logging procedures

5.4.1 Types of events recorded

HARICA Certificate Systems log all transactions related to certificate applications, issuance or revocations of certificates, issuance of CRLs, issuance or revocations of CA Certificates and all information exchanged with the Registration Authority. Furthermore, all HARICA PKI servers, log operating system processes, authentication attempts, HTTP connections to web servers, etc.

More specifically, HARICA and each Delegated Third Party SHALL record events related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems. HARICA and each Delegated Third Party SHALL record events related to 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. HARICA SHALL make these records available to its Qualified Auditor as proof of HARICA's compliance with this CP/CPS.

HARICA SHALL record at least the following events:

1. 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 sections 4.9 and 4.10); and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in 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 sections 4.9 and 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).

3. 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 SHALL include at least the following elements:

1. Date and time of event;
2. Identity of the person making the journal record (when applicable); and
3. Description of the event.

All systems that record logs are synchronized via NTP (Network Time Protocol).

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 audit log

All transactions are archived daily.

5.4.3 Retention period for audit log

HARICA and each Delegated Third Party SHALL retain, for at least **two (2)** years:

1. CA certificate and key lifecycle management event records (as set forth in section 5.4.1 (1)) after the later occurrence of:
    1. the destruction of the CA Private Key; or
    2. 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;
2. Subscriber Certificate lifecycle management event records (as set forth in section 5.4.1 (2)) after the expiration of the Subscriber Certificate;
3. Any security event records (as set forth in section 5.4.1 (3)) after the event occurred.

The transactions-events files are kept for **two (2)** years to be available for any lawful control. This period may be modified depending on developments of relevant laws.

Events that are related to Certificate lifecycle, policy/procedure documents, Key ceremonies are archived and retained per section 5.5.2.

5.4.4 Protection of audit log

Access to the transactions file in general is prohibited. Only reading and addition by authorized systems and authorized personnel is allowed. Deletion of file entries is not allowed. Multiple copies of audit logs are stored in different locations and protected by appropriate physical and logical access controls.

5.4.5 Audit log backup procedures

A backup of the transactions-events file is kept in different location in read-only mode, protected by appropriate physical and logical access controls.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

HARICA 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 caused by these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management processes; and
3. assesses the adequacy of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Periodic Penetration Tests, at least annually, and quarterly Vulnerability Scans are conducted by a highly skilled security team with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

5.5 Records Archival

5.5.1 Types of records archived

All records of transactions referred to in section 5.4, and all documentation related to requests for issuance / revocation of digital certificates are confidentially archived.

HARICA and each Delegated Third Party SHALL archive all audit logs (as set forth in section 5.4.1).

Additionally, HARICA and each Delegated Third Party SHALL archive:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention period for archive

Archived audit logs (as set forth in section 5.5.1) SHALL be retained for a period of at least

- **Seven (7) years** for "Qualified Certificates for electronic signatures/seals",
- **two (2) years** for SSL/TLS, Code Signing and non-qualified Client Certificates
- **one (1) year** for Time-Stamping Certificates

from their record creation timestamp, or as long as they are required to be retained per section 5.4.3, whichever is longer.

Additionally, HARICA and each Delegated Third Party SHALL retain, for at least two (2) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in section 5.5.1); and
2. 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:
    a. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or

b. the expiration of the Subscriber Certificates relying upon such records and documentation.

These retention periods shall be modified according to the relevant data protection laws.

5.5.3 Protection of archive

Access to the records file in general is prohibited. Only reading by authorized systems and authorized personnel is allowed. No changes or cancellations of the records of the file are allowed.

5.5.3.1 Access

Only authorized personnel may access the records file.

5.5.3.2 Protection against the alteration of the records file

An access policy which does not allow changes is applied.

5.5.3.3 Protection against the deletion of the records file

An access policy which does not allow deletions is applied.

5.5.3.4 Protection against the deterioration of storage media

Before deterioration of long-term storage media using obsolete technology, data will need to be transferred to long term storage media using more recent technology, possibly using a different cryptosystem, such that the media is protected from deterioration.

In any case, new data shall be transferred and stored in an encrypted form, and the old data shall be destroyed.

5.5.3.5 Protection against future lack of availability of readers of the old media

No stipulation.

5.5.4 Archive backup procedures

A backup of the records files is kept.

5.5.5 Requirements for time-stamping of records

Currently, the digital time stamping (in respect to RFC 3161) of the records files is not required. All files include the date and time from a trusted time source as described in section 6.8.

5.5.6 Archive collection system (internal or external)

HARICA uses an internal collection system for archive collection. Each backup added to the archive is encrypted for confidentiality and signed to maintain integrity.

5.5.7 Procedures to obtain and verify archive information

HARICA periodically verifies the integrity of the archive information by performing restore operations and signature verification of the stored archives.

5.6 Key changeover

In case a certification authority key is changed, the unexpired end-entity certificates must be revoked and re-created per the procedures in section 4.1.

HARICA will make sure that when Subordinate CA Certificates reach their expiration lifetime, they will stop issuing new certificates and will be replaced with new Subordinate CA Certificates. Previous Subordinate CA Certificates will remain in the PKI until all end-entity certificates are expired or revoked.

Root Certificates will be replaced with new rollover Roots and will be distributed to relying parties and Application Software Suppliers according to section 6.1.4.

5.7 Compromise and disaster Recovery

5.7.1 Incident and compromise handling procedures

HARICA system and application logs are periodically monitored to detect security breaching attempts or breaches of the Certificate System. If an anomaly or a suspected violation is detected, the service is suspended and a thorough check of all Certificate Systems takes place. An incident handling procedure is documented internally. This procedure includes steps for the public or confidential disclosure of security-related incidents to Application Software Suppliers.

HARICA ensures compliance with all applicable requirements (legal, statutory or else) for protecting records from violation, loss, destruction or falsification, in accordance with applicable legislation, including data protection laws, EU Regulations and related European standards.

For Publicly-Trusted server TLS and S/MIME certificates, HARICA SHALL follow the Incident Response Guidelines (IRG) published in CCADB https://www.ccadb.org/cas/incident-report. HARICA shall adopt the latest version of the CCADB IRG within 30 days of its effective date.

Incident reports SHALL include a description of the incident and be submitted within the following timelines:

- incidents involving the loss of confidentiality, integrity, or unplanned availability issues of a CA system to include components with access to CA private key material, the ability to issue and/or manage certificates, or provide certificate status information, that prevents HARICA from satisfying the commitments required by this CP/CPS, SHALL be reported within 24 hours of initial identification or notification by an external party.
- all other incidents SHALL be reported within seven (7) calendar days of initial identification or notification by an external party, whichever comes first.

HARICA is not required to publicly disclose its business continuity plans but SHALL make its business continuity plan and security plans available to its Qualified Auditor.

5.7.1.1 Mass Revocation Plans

HARICA maintains a comprehensive and actionable plan for mass revocation events, tested annually. HARICA also monitors public incidents related to delayed revocation and applies lessons learned in its internal plan to continually improve the plan over time.

HARICA's mass revocation plan includes clearly defined, actionable, and comprehensive procedures designed to ensure rapid, consistent, and reliable response to large-scale certificate revocation scenarios. HARICA is not required to publicly disclose its mass revocation plan or procedures but SHALL make them available to its auditors upon request. HARICA SHALL annually test, review, and update the mass revocation plan and corresponding procedures.

At a minimum, the mass revocation provisions SHALL include:

1. Activation criteria – specific, objective, and measurable thresholds at which the mass revocation plan is triggered based on HARICA's risk profile, issuance volumes, and operational capabilities;
2. Customer contact information – how subscriber and customer contact details are stored, maintained, and kept up to date;
3. Automation points – processes that are automated or could be automated, and those processes that require manual intervention;
4. Targets and timelines – for incident triage, revocation initiation, certificate replacement, and post-event review;
5. Subscriber notification methods – mechanisms for notifying impacted Subscribers;
6. Role assignments – roles and responsibilities of personnel responsible for initiating, coordinating, and executing the plan;
7. Training and education – training, awareness, and readiness activities for personnel responsible for, or supporting, the plan;
8. Plan testing – annual operational testing to assess readiness and demonstrate implementation feasibility, using one or more of tabletop exercises, simulations, parallel testing, or controlled test environments that DO NOT involve the revocation of active Subscriber Certificates; and
9. Post-test analysis and update schedule – how lessons learned from testing or live incidents are incorporated into the plan, and how often it is reviewed and updated.

5.7.2 Computing resources, software and/or data are corrupted

In case of suspected violation, the service is suspended and a thorough check of all Certificate Systems takes place. If a violation is confirmed, a check is done whether there is breach on CA private keys. In case of violation without CA private key compromise, the affected system is restored from backups where there is no suspicion of violation, new security checks take place to find potential security vulnerabilities and then the service returns online. In case of CA key compromise, the procedures of section 5.7.3 are followed.

5.7.3 Private key compromise procedures

In case of private keys compromise or compromise of the algorithms and parameters used to generate private keys that correspond to end-entity certificates, all related subscriber/device certificates are revoked by the certification authority and new keys and certificates are issued without interruption of the service.

In case a Private Key, associated with a Subordinate CA Certificate, is compromised, all Subscribers of the corresponding Subordinate CA are notified, all Subscriber certificates issued by the compromised Certification Authority are revoked, along with the CA Certificate.

If the private key of the Root Certification Authority is compromised, all CAs SHALL stop their service, notify all Subscribers, proceed with the revocation of all certificates, issue a final CRL and then notify the relevant security and supervisory authorities. Then the Public Key Infrastructure will be set up again with new Certification Authorities starting with a new Root Certification Authority.

5.7.4 Business continuity capabilities after a disaster

HARICA has a plan to operate continuously using backups of all Certificate Systems in a location outside the main premises of HARICA servers per a business continuity plan. The business continuity plan includes:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan,
6. Awareness and education requirements,
7. The responsibilities of the individuals,
8. Recovery time objective (RTO),
9. Regular testing of contingency plans,
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes,
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
12. What constitutes an acceptable system outage and recovery time,
13. How frequently backup copies of essential business information and software are taken,
14. The distance of recovery facilities to the CA's main site, and
15. 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.

Disaster recovery procedures are being tested, reviewed and updated annually.

Following a disaster, appropriate measures are taken to avoid repetition.

5.8 Certification Authority or Registration Authority termination

In case of a planned termination decision, HARICA will provide a timely notice to all Subscribers to switch to another Trust Service Provider. When the termination time is reached, with the exception of Short-term certificates, each Subordinate CA Operator will revoke all issued certificates, update the relevant CRL and revoke its own certificate. This revocation process includes all TSU Certificates and its Issuing CA Certificate. Furthermore, it informs the appropriate authorities and announces the end of its operation. In any case, the local and European legislation on the termination of Certification Authorities is followed.

In case of a transfer of HARICA operations to another Qualified TSP, a thorough migration and termination plan is already in place and will be implemented. All Subscribers will receive due notice of this transfer and decide whether they wish to switch to another TSP or not. During the transfer, all critical operations are expected to continue to function properly. Log files, validation evidence and all evidence associated with CA, RA and VA operations shall be transferred to the destination Qualified TSP.

In either case, the CA/RA archived files relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is kept for the retention period defined in section 5.5.2, starting at the expiration date of the Certificate. These retention periods shall be modified according to the relevant data protection laws.

When another cross-certified TSP stops all operations, including handling revocation, all cross-certificates issued under section 3.2.6 shall be revoked.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA and TSU Key Pair Generation

CA Key Pairs are generated in a secure environment, in special cryptographic devices (Hardware Security Modules or HSMs). These cryptographic devices SHALL comply with the hardware standards defined in section 6.2.7.1. TSU Key Pairs are also generated in a secure environment by personnel in trusted roles under, at least, dual control and must comply with the hardware standards defined in section 6.2.7.2.

Checks must be performed during the creation of the keys to identify the existence of bugs in software or hardware used, involving the creation of keys.

For a CA Key Pair generation and CA Certificate or TSU Certificate issuance, a well-defined key generation ceremony takes place, witnessed by an authorized committee. Especially for a CA Key Pair generation to be associated with either a Root CA Certificate or a Subordinate CA Certificate to be operated by an Externally Operated Subordinate CA, the process is witnessed by an external Auditor or the CA Key Pair generation process is recorded and sent to an external Auditor who issues an appropriate report opinion.

HARICA SHALL ensure that a Root CA Certificate submitted for inclusion in an Application Software Supplier Root Store will include a key that has been generated within five (5) years of the inclusion request.

6.1.1.2 RA Key Pair Generation

No stipulation

6.1.1.3 Subscriber Key Pair Generation

Applicant keys are generated by hardware and software at the Applicant's side or at a remote signature creation device and remain under their sole control throughout their period of validity. If the procedures of a Certification Authority allow the mass creation of keys for third parties, there must be a procedure for the destruction of all copies of the private keys after their delivery to the users for the private keys to be under the possession of the recipient Subscribers only.

If the Subscriber Certificate will contain an `extKeyUsage` extension containing either the values `id-kp-serverAuth` [RFC5280] or `anyExtendedKeyUsage` [RFC5280], HARICA SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by HARICA.

Especially, in case an Applicant wishes to obtain a "Class A" certificate, as described in section 3.2.3.1, the Applicant must:

- submit the application under the supervision of an authorized person of the Registration Authority to attest that the key generation takes place in a Hardware Crypto Module as defined in section 6.2.7.4;
- provide an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with “Class A” Certificates;
- receive a crypto-token hardware device as defined in section 6.2.7.4 that contains pre-generated Keys generated by authorized HARICA staff members operating in a Trusted Role capacity, following the process described in section 6.2.7.4;
- use a HARICA prescribed crypto library and a suitable Hardware Crypto Module combination for the Key Pair generation and storage; or
- use cryptographically verified “key attestation” to show that a certain asymmetric key has been generated on device and not imported.

Subscribers may use remote signature creation devices or a third party managing the secure cryptographic hardware device on behalf of the signer. In this case:

1. the key activation must rely on at least a 2-factor authentication (2FA) process;
2. no duplication of the private key is allowed, except for duly documented service availability purpose, and the duplicated key must abide at least the same security measures as the original;
3. the third party must disclose to HARICA the documentation (technical, procedural and operational) on the management of the secure cryptographic hardware device;
4. the third party agrees on an annual verification of the conformity of the service with its Certification Policy and/or Certificate Practice Statement, or must be certified against standards like the CEN EN 419 241 series or equivalent from an Accredited Conformity Assessment Body.

HARICA SHALL generate a Key Pair on behalf of a Subscriber for Keys that are to be associated with remote Qualified Signature/Seal Certificates, using remote QSCD certified solutions.

HARICA SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in section 6.1.5 and/or section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. HARICA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The CA has previously been notified that the Applicant's Private Key has suffered a Key Compromise using the CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted at least the following precautions SHALL be implemented:
    i. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), HARICA SHALL reject 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 Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, HARICA SHALL reject Debian weak keys.

ii. In the case of ROCA vulnerability, HARICA SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.

iii. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), HARICA SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

6.1.2 Private Key delivery to Subscriber

HARICA SHALL NOT generate a Key Pair on behalf of a Subscriber for Keys that are to be associated with SSL/TLS server Certificates, but may do so for other Certificate types.

When creating private keys on behalf of another entity, the following or stricter procedure must take place:

- If HARICA or a subCA has enough information to confirm the identity of a user in advance, it has the ability to generate a key pair and a certificate for this user.
- The identity verification is implemented when owners receive the credentials (certificate and keys) from the RA. This model is called "collective".
- HARICA or a subCA must have a procedure to delete the secret key associated with each certificate the moment it is delivered to the Subscriber, so that eventually, the private key is in possession of the Subscriber only.
- If HARICA or a subCA become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

Subscriber Private Keys may be generated and delivered to Subscribers via a hardware crypto-token. In this case:

1. HARICA shall ensure that the Subscriber's Key Pair is generated in the crypto-token
2. HARICA shall take reasonable measures to protect the crypto-token from activation, compromise, or modification during the delivery process
3. The Subscriber must acknowledge receipt of the crypto-token, and
4. HARICA must deliver the crypto-token in a way that ensures that the correct tokens and activation data are provided to the correct Subscriber
5. HARICA shall deliver activation data to the Subscriber using a separate secure channel.

Private Keys may be delivered to Subscribers in an encrypted form. If the private key is distributed in a PKCS#12 form, it shall be delivered through a secure

communications channel. If a PKCS#12 file is distributed via a physical data storage device, then:

- The storage must be packaged in a way that the opening of the package causes irrecoverable physical damage (e.g. a security seal); and
- The PKCS#12 file must have a sufficiently secure password, and the password must not be transferred together with the storage.

Third parties SHALL NOT archive the Subscriber's Private Key without authorization by the Subscriber.

6.1.3 Public key delivery to certificate issuer

The Applicant must submit the public key to the Registration Authority through a structured Certificate Signing Request (PKCS#10). This request is signed with the relevant private key. More information is available in section 3.2.1.

6.1.4 CA public key delivery to relying parties

HARICA ROOT Certificates are mainly distributed via Application Software Suppliers through appropriate Root CA Programs (for example Microsoft, Apple, Mozilla). HARICA Subordinate CA Certificates, are available for secure download via the HARICA certificate repository described in section 2.1. CA Certificates can also be found in the European Union's Trusted List of Certification Service Providers via the National Supervisory Authority (Hellenic Telecommunications & Post Commission). TSA and TSU Certificates are also distributed via the EU Trusted List via the Greek Supervisory Authority (EETT). Other delivery procedures include traditional postal mail delivery and transmission of the corresponding fingerprints via an alternative communication channel.

6.1.5 Key sizes

For RSA key pairs HARICA SHALL:

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

For RSA key pairs that are to be associated with Code Signing and Time-Stamping Certificates, the modulus size, when encoded, must be at least 3072 bits.
Effective 2025-12-31, for RSA key pairs to be associated with Qualified Certificates, the modulus size, when encoded, shall be at least 3000 bits.

For EdDSA key pairs, HARICA SHALL:

- ensure that the key represents a valid point on the curve25519 or curve448 elliptic curve.

For ECDSA key pairs, and only in association with S/MIME or signature Certificates, HARICA SHALL:

- ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

For ML-DSA key pairs, the CA SHALL:

• Ensure the Key uses one of the following parameter sets:

- ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17), or
- ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18), or
- ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19).

For ML-KEM key pairs, the CA SHALL:

• Ensure the Key uses one of the following parameter sets:

- ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or
- ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
- ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3).

CAs that issue certificates with the `id-kp-codeSigning` KeyPurposeId in the `extKeyUsage` extension, SHALL chain up to a CA with a minimum of RSA 4096-bit modulus or ECC NIST-P384 and SHALL support the SHA2 hash algorithms.

Key Pairs are generated using secure algorithms and parameters based on current research and industry standards following the recommendations of ETSI TS 119 312.

6.1.6 Public key generation parameters and quality checking

Public key generation parameters can be selected by Applicants which are verified by the Registration Authority and the Certification Authority. Key Pairs are generated using secure algorithms and parameters based on current research and industry standards following the recommendations of ETSI TS 119 312.

For RSA Keys, HARICA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus SHOULD also have 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]

For ECDSA Keys, HARICA, where technically feasible, confirms the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2].

For EdDSA key pairs: no stipulation.

For ML-DSA key pairs: no stipulation.

For ML-KEM key pairs: no stipulation.

HARICA performs quality checks for the keys to be included in issued Certificates during the issuance process. See also section 6.1.1.3.

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

Private Keys corresponding to Root Certificates SHALL NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

The intended use of a key is referred by the designated basic field and the designated extension of the X509v3 type of certificate. The certificate usage purposes are not restrictive (e.g. non-critical certificate extension) but "suggested". Monitoring compliance with the authorized purposes usage is at the discretion of relevant parties.

More information about certificate extensions is available in section 7.1.2.

A list of the most common certificate profiles used by HARICA are listed in ANNEX B (HARICA Common Certificate Profiles).

6.2 Private key protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Cryptographic module standards and controls for Private Key generation and protection are described in section 6.2.7.

6.2.2 Private Key control from multiple persons (N out of M)

The activation of the private key of every CA (including backups) follows the procedures described in section 5.2.2.

6.2.3 Private Key escrow

HARICA does not currently offer Key escrow services.

6.2.4 Private Key backup

The private key of every CA SHALL be kept at a backup copy. TSU private keys MAY be backed up. CA and TSU Private Key backups must be encrypted, and the procedures referenced at section 5.1.6 must be followed. Only authorized personnel occupying a Trusted Role have access to the backup copy. Restoring CA and TSU backup keys require dual control in a physically secured environment. Any backup copies of the CA or TSU private signing keys shall be protected to ensure its integrity and confidentiality by the cryptographic module before being stored outside that device.

Private key backup for Subscriber certificates (if such an action is technically feasible), is exclusively under the control of the Subscriber.

6.2.5 Private Key archival

The backup copy of the private key of each CA and TSU must be archived and kept using secure methods at a secure place. Private keys at the backup copy are always encrypted. Furthermore, all procedures at section 5.1.6 are followed. Access to the archived backup copy is allowed only by authorized personnel.

CA Private Keys shall not be archived by Third Parties.

All copies of the CA and TSU private signing keys are put beyond use at the end of their life cycle.

6.2.6 Private Key transfer into or from a cryptographic module

Owners of private keys may transfer their private key from a software certificate store to any hardware cryptographic device, e.g. crypto-tokens, smartcards. This procedure does not change the class of the certificate from B to A since the private key was not generated originally on the hardware cryptographic device. The reverse procedure (transfer of the private key from a hardware device to a software certificate store) is not allowed.

All transfers of CA Private Keys into or from an HSM are performed in accordance with the procedures specified by the vendor of the HSM.

If the Issuing CA generated the Private Key on behalf of a Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA.

If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key storage on cryptographic module

6.2.7.1 Private key storage for CA keys

All CA and TSU private keys SHALL be stored in a secure Hardware Security Module to perform key signing operations. HARICA SHALL protect CA Private Keys in a system or device that has been validated as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

HARICA may use non-certified solutions to store CA keys with the ML-DSA algorithm during an experimental phase, until HARICA's HSMs become certified supporting Quantum-safe algorithms.

6.2.7.2 Private key storage for Timestamp Authorities

A Timestamp Authority SHALL protect its signing key using a process that is at least to FIPS 140-2 Level 3, Common Criteria EAL 4+ (ALC_FLR.2), or higher.

6.2.7.3 Private key storage for Signing Services

The Signing Service SHALL ensure that a Subscriber's Private Key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. A Signing Service SHALL enforce multi-factor authentication to access and authorize Code Signing and obtain a representation from the Subscriber that they will securely store the tokens required for multi-factor access. A system used to host a Signing Service SHALL NOT be used for web browsing. The Signing Service SHALL run a regularly updated antivirus solution to scan the service for possible virus infection. The Signing Service SHALL comply with the Network Security Guidelines as a "Delegated Third Party".

For Code Signing Certificates, Signing Services shall protect Private Keys in a Hardware Crypto Module conforming to at least FIPS 140-2 level 2 or Common Criteria EAL 4+.

Techniques that MAY be used to satisfy this requirement include:

1. Use of an HSM, verified by means of a manufacturer's certificate;
2. A cloud-based key generation and protection solution with the following requirements: a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution’s Hardware Crypto Module that conforms to the specified requirements; b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
3. A Hardware Crypto Module provided by the CA;
4. Contractual terms in the Subscriber Agreement requiring the Subscriber to protect the Private Key to a standard of at least FIPS 140-2 level 2 or Common Criteria EAL 4+ and with compliance being confirmed by means of an audit.

For Qualified Signature/Seal Certificates, Signing Services shall protect Private Keys in a remote QSCD certified solution.

6.2.7.4 Subscriber Private Key protection and verification

6.2.7.4.1 Subscriber Private Key protection

Subscriber Private Keys for Code Signing Certificates SHALL be protected per the following requirements. HARICA SHALL obtain a contractual representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

7. Subscriber uses a Hardware Crypto Module meeting the specified requirement;

8. Subscriber uses a cloud-base key generation and protection solution with the following requirements:
    a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
    b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
9. Subscriber uses a Signing Service which meets the requirements of section 6.2.7.3.

Only **Qualified Signature/Seal Creation Devices** shall be used for the creation of Key Pairs associated with Certificates for **Qualified Electronic Signatures/Seals**.

Special controls must be in place to ensure that any cryptographic hardware used has not been tampered with and is functioning correctly. The integrity of the hardware and software used for key generation, and of any interfaces used to access the hardware and software, is tested before production usage.

In the special case of Qualified Certificates with Qualified Signature/Seal Creation Device (QSCD) (Class A Certificates), the Private Key SHALL be generated and stored in a QSCD and cannot be extracted in any form. QSCD devices SHALL meet at least FIPS PUB 140-2 level 3 or equivalent EAL 4+ or higher in accordance to ISO/IEC 15408 specifications.

HARICA monitors relevant information for QSCD certifications using an informative list of certified QSCDs from the European Commission based on Article 31 of eIDAS:

- https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

For remote QSCDs that manage Private Keys on behalf of the Subscriber, HARICA monitors compliance with the applicable Common Criteria security target of the remote QSCD. Such Certificates include an additional policy OID according to section 7.1.6.

6.2.7.4.2 Subscriber Private Key verification

For Code Signing Certificates, HARICA SHALL ensure that the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in 6.2.7.4.1. One of the following methods SHALL be employed to satisfy this requirement:

1. HARICA ships a suitable Hardware Crypto Module, with one or more pre-generated Key Pairs that the CA has generated using the Hardware Crypto Module;
2. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Module;

3. The Subscriber uses a HARICA prescribed crypto library and a suitable Hardware Crypto Module combination for the Key Pair generation and storage;
4. The Subscriber provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates;
5. The Subscriber provides a suitable report from a cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware Crypto Module;
6. HARICA relies on a report provided by the Applicant that is signed by an auditor who is approved by HARICA and who has IT and security training or is a CISA, witnesses the Key Pair creation in a suitable Hardware Crypto Module solution including a cloud-based key generation and protection solution;
7. The Subscriber provides an agreement that they use a Signing Service meeting the requirements of section 6.2.7.3.

6.2.8 Methods of activating private key

6.2.8.1 Who can activate (use) a private key

To activate a CA key, only a combination of authorized users can perform a "CA Activation procedure", which is described in an internal HARICA document. After the activation of the keys in the HSM, the corresponding CAs can perform cryptographic procedures.

The private keys that correspond to Subscriber certificates, should be protected-encrypted. The owner of each certificate is responsible to enable and protect the private key that corresponds to the certificate.

6.2.8.2 Actions to be performed to activate a private key

For CA private key activation that is stored in HSMs, a combination of authentication/authorization tokens is required. Each authorized key activation member, holds a different token necessary for the activation procedure. Only a combination of the authorized key activation members can activate a private key.

For Subscriber private key, in case of hardware cryptographic device (e.g. crypto-tokens) a specific PIN is required. If Subscriber private keys are stored in software certificate stores (e.g. CryptoAPI at MS Windows), a passphrase may not be required but a simple question of whether to use the private key. Finally, private keys used in devices-services may be permanently activated and not protected at all using a passphrase, if there are other sufficient security measures at the file system level (file system permissions) or other equivalent security precautions.

6.2.8.3 Once activated, for how long is the key "active"?

Usually the key stays "active" for a limited time in which the application that uses the certificate, is active.

For the key associated with a ROOT CA Certificate, the key remains "active" only for the time required to perform cryptographic operations e.g. Subordinate CA Certificate signing/revocation, OCSP Certificate signing, OCSP pre-signed responses, or CRL generation operations.

6.2.9 Methods for deactivating private key

No stipulation.

6.2.10 Methods for destroying private key

Once a CA Certificate reaches the end of its lifetime, the private key is "destroyed" using the secure deletion procedure of the Hardware Security Module with instructions from the HSM manufacturer, under dual control methods as described in section 5.2.2. This "destruction" affects only the physical instance of the key stored in the HSM. Other backup copies are deleted using secure deletion procedures, using the US DoD 5220.22-M secure deletion scheme or stronger.

As all backup files of CA and TSU Private Keys are encrypted using a symmetric "Master Backup Key", an additional method of destroying these encrypted backups is the destruction of the "Master Backup Key" which results in making all encrypted backups practically unusable (not able to be decrypted).

TSU Private Keys that reach the end of their validity period per section 6.3.2, shall be deleted in a way that is practically impossible to use and issue new TSTs.

Subscribers may destroy their private keys on their own.

6.2.11 Cryptographic module rating

Described in section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are embedded within the digital certificates during their issuance and are archived according to the procedures defined in section 5.4.

6.3.2 Certificate operational periods and key pair usage periods

The key pair operational period starts when a public key is first included in a digital certificate known to HARICA (via a CSR submission by the Applicant). Depending on the Certificate type, HARICA has different key pair operational periods.

The maximum operational period of the keys that are generated in HSMs or crypto-devices that meet the expectations of section 6.2.7.4 shall be:

- **twenty-five (25) years** for Root CA Certificates,
- **fifteen (15) years** for Subordinate CA Certificates,
- **ten (10) years** for Client Authentication, Code Signing, Document Signing and S/MIME Certificates,

- **ten (10) years** for a Time-Stamping Unit or EV Timestamp Certificate. For the case of Time-Stamping Unit, a new Time-Stamping Unit Certificate with a new private key must be created no later than **every fifteen (15) months**.

The maximum operational period of the keys that are not generated in devices that meet the expectations of section 6.2.7.4, should be **five (5) years**.

The operational period must be defined according to the size of the keys and the current technological developments at the field of cryptography, so that the best level of security and efficiency of use is guaranteed.

The maximum validity period of Certificates shall be:
- for a Root CA Certificate, **twenty-five (25) years**;
- for a Subordinate CA Certificate, **fifteen (15) years**;
- for SSL/TLS Client Authentication and Document Signing Certificates, **three (3) years**;
- for S/MIME Certificates, **eight hundred twenty-five (825) days**;
- for Code Certificates:
  - **eight hundred twenty-five (825) days** until March 1, 2026
  - **Effective** 2026-03-01, **four hundred and sixty (460) days**,
- for SSL/TLS Server Authentication Certificates:
  - **three hundred ninety-eight (398) days** until March 15, 2026,
  - **Effective** 2026-03-15, **two hundred (200) days**,
  - **Effective** 2027-03-15, **two hundred (100) days**,
  - **Effective** 2029-03-15, **two hundred (47) days**;
- for a Time-Stamping Unit Certificate, **ten (10) years**.

Short-term Certificates shall have a maximum Validity Period of **twenty-four (24) hours**.

According to OVR-6.1-7 of ETSI TS 119 495, SSL/TLS Certificates asserting the QNCP-w-gen and QCP-w-psd2 policy OIDs outside the context of a web browser, may have different maximum validity period according to the Open Banking use case.

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

The activation data (passphrases and PINs) must be chosen in such a way so that it is difficult to be discovered. The minimum size of the passphrase and the PIN is **eight (8)** characters. In case there is an embedded private key destruction mechanism after a certain number of incorrect entries, then the PIN size may be smaller. In any case, the procedures defined in section 6.2.8 are used.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

- The Operating Systems of the computers of HARICA are kept in high security level with the implementation of international standards and security guidelines.
- There are logging systems and alarm facilities at the computers operating in the HARICA PKI which are checked on a regular basis and the log files are scrutinized periodically in order to identify potential anomalies and security incidents in order to initiate response procedures. Response procedures allow the personnel to act as soon as possible in order to limit the impact of breaches of security.
- Only the absolutely necessary programs/applications for the correct operation of the RA/CA are installed within the Operating System and the computers shall be protected against malicious and unauthorized software. All programs shall be upgraded to their latest version whenever security fixes emerge that affect PKI software.
- HARICA enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

HARICA PKI software goes through secure development procedures before being published to the production environment.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

HARICA uses internal procedures to reasonably ensure that physical servers, HSMs and cryptographic modules used in critical PKI operations remain un-tampered during shipment or storage. All critical devices operate in a physically secured environment.

6.7 Network security controls

All CA/RA servers are operating behind firewalls that restrict access to only authorized servers and only to ports used for managing the CA and issuing Certificates or Timestamps. Sensitive data shall be protected when exchanged over networks using cryptographic methods to ensure their confidentiality and integrity.

HARICA follows the network security guidelines of section 7.8 of the ETSI EN 319 401. In addition, HARICA follows the security guidelines of “Network and Certificate System Security Requirements” of the CA/Browser Forum

6.8 Time-stamping

HARICA operates as a Time-Stamping Authority and performs all the necessary actions for the uninterruptible - as possible - availability of its Time-Stamping service.

6.8.1 Time-Stamp Issuance

Time-stamps shall conform to the time-stamp profile as defined in ETSI EN 319 422 and shall be issued securely and include the correct representation of time, in sync with UTC.

If the TSU's clock is detected as being out of the stated accuracy, then time-stamps shall not be issued until the clock is synced with the stated accuracy.

Time-stamps shall be signed using a key generated exclusively for this purpose associated with a TSU Certificate.

Time-stamps should not be produced when the end of the validity of the TSU Private Key has been reached.

6.8.2 Time-Stamping Unit

TSUs operated by HARICA must have a single time-stamp signing key active at a time. The validity of the private key used to sign TSTs is defined in section 6.3.2.

TSU signature verification (public) keys are available to relying parties in a public key certificate using the timestamping EKU (section 7.1.2 and Annex B).

TSUs shall correspond to a Key Pair generated exclusively for the purpose of Time Stamping.

TSUs shall use SHA2 hashing algorithms to represent the datum being time-stamped.

HARICA shall use separate service access points and different TSUs identified by different subject names in their public key certificate to distinguish signed Qualified Time-Stamps from non-Qualified Time-Stamps.

6.8.3 Time-Stamp Token

TSTs signed by HARICA TSUs are issued securely and include accurate representation of time in sync with UTC. The time values the TSU uses in the time-stamp shall be traceable to at least one of the real-time values distributed by a UTC(k) laboratory.

Each TST follows the requirements of ETSI EN 319 422 and includes:

- `policy` identifier for the time-stamp policy per section 7.1.8;
- a `genTime` field shall have a value representing time with the precision necessary to support the declared accuracy;
- `accuracy` field with a minimum accuracy of **one (1) second** compared to UTC, traceable to a UTC(k) source;
- a unique serial number for each TST;

- an electronic signature generated using a key used exclusively for time-stamping; and
- a `signerInfo` attribute for the identification of the TSU.

6.8.4 Clock synchronization with UTC

The following requirements for clock synchronization apply:

- The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.
- If it is detected that the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC, the TSU shall stop time-stamp issuance.
- The clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body.

HARICA synchronizes and calibrates the clock continuously (at least every hour) against reference UTC time sources. In the unlikely event that the TSU clock drifts outside the declared minimum accuracy and the recalibration fails, the TSU shall stop time-stamp issuance until the clock is properly calibrated.

HARICA keeps audit logs for all UTC clock calibrations.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate profile

A certificate profile per RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile” is used.

HARICA SHALL meet the technical requirements set forth in Section 6.1.5 and section 6.1.6.

For purposes of clarification, a Pre-certificate, as described in RFC 6962 – Certificate Transparency, is not considered to be a “certificate” subject to the requirements of RFC 5280.

7.1.1 Version number

The version number of the certificates is 2, which corresponds to X.509v3 certificates.

7.1.2 Certificate Extensions

Every issued certificate includes extensions as they are defined for X.509v3 Certificates. Here is a list of extensions used by HARICA. This list is not limited.

7.1.2.1 Root CA Certificate

1. `basicConstraints`

   This extension SHALL appear and SHALL be marked critical. The `cA` field SHALL be set true. The `pathLenConstraint` field SHOULD NOT be present.

2. `keyUsage`

This extension SHALL be present and SHALL be marked critical. Bit positions for `keyCertSign` and `cRLSign` SHALL be set. If the Root CA Private Key is used for signing OCSP responses, then the `digitalSignature` bit SHALL be set.

3. `certificatePolicies`

   This extension SHOULD NOT be present.

4. `extKeyUsage`

   This extension SHALL NOT be present

7.1.2.2 Intermediate CA Certificate

1. `basicConstraints`

   This extension SHALL be present and SHALL be marked critical. The `cA` field SHALL be set true. The `pathLenConstraint` field MAY be present.

2. `authorityKeyIdentifier`

   This extension SHALL be present and SHALL NOT be marked critical. It SHALL contain a `keyIdentifier` field and it SHALL NOT contain a `authorityCertIssuer` or `authorityCertSerialNumber` field.

3. `subjectKeyIdentifier`

   This extension SHALL be present and SHALL NOT be marked critical. It identifies a particular CA Key uniquely. It contains the ID of the CA Certificate key

4. `keyUsage`

   This extension SHALL be present and SHALL be marked critical. Bit positions for `keyCertSign` and `cRLSign` SHALL be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the `digitalSignature` bit SHALL be set.

5. `certificatePolicies`

   This extension SHALL be present and SHOULD NOT be marked critical. More information about the range of asserted OIDs are explained in section 7.1.6.

   `certificatePolicies:policyIdentifier` (Required)

   A Certificate issued to a Subordinate CA that is not an Affiliate of the Issuing CA:

   1. MUST include one or more explicit policy identifiers that indicate the Subordinate CA's adherence to and compliance with this CP/CPS and
   2. MAY contain one or more identifiers documented by the Subordinate CA in its Certificate Policy and/or Certification Practice Statement and
   3. MUST NOT contain the `anyPolicy` identifier (2.5.29.32.0).

   A Certificate issued to a Subordinate CA that is an affiliate of the Issuing CA:

1. MAY include one or more explicit policy identifiers that indicate the Subordinate CA's adherence to and compliance with this CP/CPS and
2. MAY contain one or more identifiers documented by the Subordinate CA in its Certificate Policy and/or Certification Practice Statement and
3. MAY contain the `anyPolicy` identifier (2.5.29.32.0) in place of an explicit policy identifier.

The Subordinate CA and the Issuing CA SHALL represent, in their Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with this CP/CPS are issued and managed in accordance with this CP/CPS.

6. `extKeyUsage`

For Cross Certificates that share a Subject Distinguished Name and Subject Public Key with a Root Certificate operated in accordance with this CP/CPS, this extension MAY be present. If present, this extension SHOULD NOT be marked critical. This extension SHALL only contain usages for which the issuing CA has verified the Cross Certificate is authorized to assert. This extension MAY contain the `anyExtendedKeyUsage` [RFC5280] usage, if the Root Certificate(s) associated with this Cross Certificate are operated by HARICA.

For all other Subordinate CA Certificates, including Technically Constrained Subordinate CA Certificates:

This extension SHALL be present and SHOULD NOT be marked critical[4].

For Subordinate CA Certificates that will be used to issue TLS server certificates, the value `id-kp-serverAuth` [RFC5280] SHALL be present. The value `id-kp-clientAuth` [RFC5280] MAY be present. **Effective 2026-06-15**, the value `id-kp-clientAuth` [RFC5280] SHALL NOT be present for CA Certificates chaining to the Chrome Root Store. The values `id-kp-emailProtection` [RFC5280], `id-kp-codeSigning` [RFC5280], `id-kp-timeStamping` [RFC5280], `id-kp-OCSPSigning` [RFC5280] and `anyExtendedKeyUsage` [RFC5280] SHALL NOT be present. Other values SHOULD NOT be present.

For Subordinate CA Certificates that are not used to issue TLS certificates, then the value `id-kp-serverAuth` [RFC5280] SHALL NOT be present. Other values MAY be present, but SHOULD NOT combine multiple independent key purposes (e.g. including `id-kp-timeStamping` [RFC5280] with `id-kp-codeSigning` [RFC5280]).

7. `cRLDistributionPoints`

This extension SHALL be present and SHALL NOT be marked critical. It SHALL contain the HTTP URL of the CA’s CRL service.

8. `authorityInformationAccess`

[4] While RFC 5280, section 4.2.1.12, notes that this extension will generally only appear within end-entity certificates, this CP/CPS makes use of this extension to further protect relying parties by limiting the scope of subordinate certificates, as implemented by a number of Application Software Suppliers.

This extension SHOULD be present and SHALL NOT be marked critical.

It SHOULD contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2). It MAY contain the HTTP URL of the Issuing CA's OCSP responder (`accessMethod` = 1.3.6.1.5.5.7.48.1).

9. `nameConstraints` (optional)

   If present, this extension SHOULD be marked critical[5].

7.1.2.3 End-entity Certificate

1. `basicConstraints` (optional)

   The `cA` field SHALL NOT be true.

2. `authorityKeyIdentifier (required)`

   Provides information to identify the Public Key corresponding to the Private Key used to sign a Certificate. This field contains the "Subject Key Identifier" of the issuing CA's Certificate.

   This extension SHALL be present and SHALL NOT be marked critical. It SHALL contain a `keyIdentifier` field and it SHALL NOT contain a `authorityCertIssuer` or `authorityCertSerialNumber` field.

3. `subjectKeyIdentifier (not recommended)`

   Identifies a particular Public Key uniquely. It contains the ID of the Certificate Holder's key

4. `keyUsage` (optional)

   If present, bit positions for `keyCertSign` and `cRLSign` SHALL NOT be set. For Qualified Certificates for eSignature/Seal (advanced or qualified), the `nonRepudiation` bit SHALL be set.

5. `certificatePolicies`

   This extension SHALL be present and SHOULD NOT be marked critical. More information about the range of asserted OIDs are explained in section 7.1.6.

   – `certificatePolicies:policyIdentifier` (Required)

     A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with this CP/CPS.

   The following extensions MAY be present:

   – `certificatePolicies:policyQualifiers:policyQualifierId` (Not Recommended for server TLS Certificates)

     `id-qt 1` [RFC 5280].

[5] Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they MAY be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

- `certificatePolicies:policyQualifiers:qualifier:cPSuri` (Optional)

  HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

6. `extKeyUsage` (required)

   For TLS Certificates, either the value `id-kp-serverAuth` [RFC5280] or `id-kp-clientAuth` [RFC5280] or both values SHALL be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` SHALL NOT be present. **Effective 2026-06-15**, the value `id-kp-clientAuth` [RFC5280] SHALL NOT be present for server TLS Certificates chaining to the Chrome Root Store.

   For S/MIME Certificates, either the value `id-kp-emailProtection` [RFC5280] or `id-kp-clientAuth` [RFC5280] or both values SHALL be present. `MS Document Signing` (OID: 1.3.6.1.4.1.311.10.3.12), `AuthenticDocumentsTrust` (OID: 1.2.840.113583.1.1.5), or `smartcardlogon` (OID: 1.3.6.1.4.1.311.20.2.2) MAY be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` SHALL NOT be present.

   For Document Signing, eSignature or eSeal Certificates, either the value `MS Document Signing` (OID: 1.3.6.1.4.1.311.10.3.12) or `AuthenticDocumentsTrust` (OID: 1.2.840.113583.1.1.5) or id-kp-docSigning [RFC9336] or any combination of those values SHALL be present. `id-kp-emailProtection` [RFC5280], `id-kp-clientAuth` [RFC5280] or `smartcardlogon` (OID: 1.3.6.1.4.1.311.20.2.2) MAY be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` SHALL NOT be present.

   For Code Signing Certificates, the value `id-kp-codeSigning` [RFC5280] SHALL be present. `id-kp-clientAuth` [RFC5280] or `Lifetime Signing` (OID: 1.3.6.1.4.1.311.10.3.13) MAY be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` SHALL NOT be present.

   For Time-stamping Certificates, the value `id-kp-timeStamping` [RFC5280] SHALL be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` SHALL NOT be present.

   For delegated OCSP responder Certificates, the value `id-kp-OCSPSigning` [RFC5280] SHALL be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` SHALL NOT be present.

7. `cRLDistributionPoints`

For TLS Certificates, this extension MAY be present. For Client Authentication, Code Signing, S/MIME and Time-stamping Certificates, this extension SHALL be present. For Short-term Certificates used for eSignatures and eSeals, this extension MAY NOT be present.

If present, it SHALL NOT be marked critical, and it SHALL contain the HTTP URL of the CA's CRL service.

8. `authorityInformationAccess`

   For TLS and Qualified eSignature/eSeal Certificates, this extension SHALL be present. For Client Authentication, Code Signing, S/MIME and Time-stamping Certificates, this extension MAY be present. For Short-term Certificates used for eSignatures and eSeals, this extension MAY NOT be present.

   If present, it SHALL NOT be marked critical, and it SHALL contain the HTTP URL of the Issuing CA's OCSP responder (`accessMethod` = 1.3.6.1.5.5.7.48.1).

   It SHOULD also contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2).

9. `subjectAltName` (required for TLS and S/MIME Certificates)

   For TLS Certificates this extension SHALL be present and SHALL contain at least one entry. Each entry SHALL be one of the following types:

   - `dNSName`: The entry SHALL contain either a Fully-Qualified Domain Name or Wildcard Domain Name that HARICA has validated in accordance with section 3.2.2.4. Wildcard Domain Names SHALL be validated for consistency with section 3.2.2.6. The entry SHALL NOT contain an Internal Name or a Domain Name that ends in an IP Address Reverse Zone Suffix.

   The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry SHALL be composed entirely of 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 SHALL NOT be included (e.g. "example.com" SHALL be encoded as "example.com" and SHALL NOT be encoded as "example.com.").

   The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name SHALL consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.

   - `iPAddress`: The entry SHALL contain an IPv4 or IPv6 address that HARICA has validated in accordance with section 3.2.2.5. The entry SHALL NOT contain a Reserved IP Address.

   For S/MIME Certificates this extension SHALL be present and SHALL contain at least one GeneralName entry of the following types:

   - `rfc822Name` and/or
   - `otherName` of type `id-on-SmtpUTF8Mailbox`, encoded in accordance with RFC 9598.

which SHALL contain an email address that HARICA has validated in accordance with section 3.2.3. All Mailbox Addresses in the subject field or entries of type `directoryName` of this extension SHALL be repeated as `rfc822Name` or `otherName` values of type `id-on-SmtpUTF8Mailbox` in this extension.

Entries of type `directoryName` MAY be present to convey an alternative representation of the Subject Distinguished Name. If present, these entries SHALL contain subject DN attributes that HARICA has validated in accordance with section 3.2. Other types such as `otherName` or `uniformResourceIdentifier` MAY be present.

For Document Signing, eSignature or eSeal Certificates this extension MAY be present. If present, it SHALL contain at least one entry of type `directoryName` to convey an alternative representation of the subscriber's Distinguished Name. If present, these entries SHALL contain subject DN attributes that HARICA has validated in accordance with section 3.2. Other types such as `otherName` or `uniformResourceIdentifier` MAY be present.

10. `qcStatements` (1.3.6.1.5.5.7.1.3) (required for Qualified Certificates)

    If the Certificate is used in compliance with eIDAS, this extension contains special attributes/values to convey information to Relying Parties. The value "`id-etsi-qcs-QcCompliance`" specifies that the certificate is a Certificate for electronic signatures/seals per eIDAS and SHALL always be present in Certificates for Advanced/Qualified electronic signatures/seals. Additionally, Certificates for Qualified electronic signatures/seals SHALL include the value "`id-etsi-qcs-QcSSCD`", which asserts that the private key was generated in an SSCD/QSCD. Additional values are allowed and SHALL follow the requirements described in ETSI EN 319 412-1.

    If the Certificate is used in compliance with Regulation (EU) No. 2018/389 and Directive (EU) 2015/2366, the `qcStatements` extension may contain special attributes/values in a `etsi-psd2-qcStatement` to convey information about Payment Service Providers to Relying Parties. In this case, the statement SHALL follow the requirements described in ETSI TS 119 495, and must contain:
    - the role of the payment service provider, which may be one or more of the following:
      - account servicing (PSP_AS);
      - payment initiation (PSP_PI);
      - account information (PSP_AI);
      - issuing of card-based payment instruments (PSP_IC)
    - the name of the competent authority where the payment service provider is registered.

11. `cabfOrganizationIdentifier` (OID: 2.23.140.3.1) (required for EV TLS Certificates using the `subject:organizationIdentifier` attribute)

    If the Certificate is asserting the EVCP or QEVCP-w certificate policy OID (see section 7.1.6) and the `subject:organizationIdentifier` field is present, this

field SHALL be present in a special CA/Browser Forum extension. This extension shall follow the requirements of sections 7.1.4.8 and 7.1.2.2 of the EV Guidelines.

12. `ext-etsi-valassured-ST-certs` (OID: 0.4.0.194121.2.1)

    If the Certificate is asserting to be a Short-term Certificate, it should use the validity assured extension `ext-etsi-valassured-ST-certs` defined in ETSI EN 319 412-1 within the Short-term Certificates which cannot be revoked.

7.1.2.4 All Certificates

All other fields and extensions SHALL be set in accordance with RFC 5280. For purposes of clarification, a Precertificate, as described in RFC 6962 - Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under this CP/CPS. HARICA SHALL NOT issue a Certificate that contains a keyUsage flag, extKeyUsage value, Certificate extension, or other data not specified in section 7.1.2.1, section 7.1.2.2, or section 7.1.2.3 unless HARICA is aware of a reason for including the data in the Certificate.

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

1. SHALL apply in the context of the public Internet, unless:
    a) the extension OID falls within an OID arc for which the Applicant demonstrates ownership, or
    b) the Applicant can otherwise demonstrate the right to assert the data in a public context.
2. SHALL NOT include semantics that will mislead Relying Parties about certificate information verified by HARICA (such as including an extension that indicates a Private Key is stored on a smart card, where HARICA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

HARICA SHALL NOT include additional extensions or values unless HARICA is aware of a reason for including the data in the Certificate. A list of the most common certificate profiles used by HARICA are listed in ANNEX B (HARICA Common Certificate Profiles).

7.1.3 Algorithm Object Identifiers

The signature algorithms SHALL follow the specifications described in sections 6.1.5 and 6.1.6. All algorithms used for CAs, Subscriber and TSU Certificates, must follow current research and industry standards to deliver reasonable security for the intended purposes they are being used.

7.1.3.1 SubjectPublicKeyInfo

For SSL/TLS Certificates, the following requirements apply to the subjectPublicKeyInfo field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

HARICA SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters SHALL be present, and SHALL be an explicit NULL. HARICA SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

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

7.1.3.1.2 ECDSA

HARICA SHALL indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters SHALL use the `namedCurve` encoding.

- For P-256 keys, the `namedCurve` SHALL be `secp256r1` (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the `namedCurve` SHALL be `secp384r1` (OID: 1.3.132.0.34).
- For P-521 keys, the `namedCurve` SHALL be `secp521r1` (OID: 1.3.132.0.35).

When encoded, the AlgorithmIdentifier for ECDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For P-256 keys, `301306072a8648ce3d020106082a8648ce3d030107`.
- For P-384 keys, `301006072a8648ce3d020106052b81040022`.
- For P-521 keys, `301006072a8648ce3d020106052b81040023`.

7.1.3.1.3 EdDSA

HARICA SHALL indicate an EdDSA key using one of the following algorithm identifiers below:

- For curve25519 keys, the algorithm SHALL be id-Ed25519 (OID: 1.3.101.112).
- For curve448 keys, the algorithm SHALL be id-Ed448 (OID: 1.3.101.113).

The parameters for EdDSA keys SHALL be absent.
When encoded, the AlgorithmIdentifier for EdDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For Curve25519 keys, 300506032b6570.
- For Curve448 keys, 300506032b6571.

7.1.3.1.4 ML-DSA

HARICA SHALL indicate an ML-DSA key using one of the following algorithm identifiers below:

- ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17), or
- ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18), or
- ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19).

The parameters for ML-DSA keys SHALL be absent. HARICA MUST NOT use HashML-DSA; only "pure" ML-DSA is permitted.
When encoded, the AlgorithmIdentifier for ML-DSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-DSA-44, 300b06096086480165030403 11.
- For ML-DSA-65, 300b06096086480165030403 12.
- For ML-DSA-87, 300b06096086480165030403 13.

7.1.3.1.5 ML-KEM

HARICA SHALL indicate an ML-KEM key using one of the following algorithm identifiers below:

- ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or
- ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
- ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3).

The parameters for ML-KEM keys SHALL be absent.
When encoded, the AlgorithmIdentifier for ML-KEM keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-KEM-512, 300b06096086480165030404 01.
- For ML-KEM-768, 300b06096086480165030404 02.
- For ML-KEM-1024, 300b06096086480165030404 03.

7.1.3.2 Signature AlgorithmIdentifier

For SSL/TLS Certificates, all objects signed by a CA Private Key SHALL conform on the use of the `AlgorithmIdentifier` or `AlgorithmIdentifier`-derived type in the context of signatures. It applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate or Precertificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

HARICA SHALL use one of the following signature algorithms and encodings. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:
  Encoding: `300d06092a864886f70d01010b0500`.
- RSASSA-PKCS1-v1_5 with SHA-384:
  Encoding: `300d06092a864886f70d01010c0500`.
- RSASSA-PKCS1-v1_5 with SHA-512:
  Encoding: 300d06092a864886f70d01010d0500.
- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:
  Encoding:
  `304106092a864886f70d01010a3034a00f300d06096086480165030402 01`
  0500a11c301a06092a864886f70d010108300d06096086480165030402 01
  0500a203020120
- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:
  Encoding:

304106092a864886f70d01010a3034a00f300d06096086480165030402020500a11c301a06092a864886f70d010108300d060960864801650304020205
00a203020130

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:
  Encoding:
  304106092a864886f70d01010a3034a00f300d06096086480165030402030500a11c301a06092a864886f70d010108300d060960864801650304020305
  00a203020140

In addition, HARICA MAY use the following signature algorithm and encoding

- RSASSA-PKCS1-v1_5 with SHA-1:
- Encoding: `300d06092a864886f70d0101050500`

if all the following conditions are met:

- If used within a Certificate, such as the `signatureAlgorithm` field of a Certificate or the `signature` field of a TBSCertificate:
  - The new Certificate is a Root CA Certificate or Subordinate CA Certificate that is a Cross-Certificate; and,
  - There is an existing Certificate, issued by the same issuing CA Certificate, using the following encoding for the signature algorithm; and,
  - The existing Certificate has a `serialNumber` that is at least 64-bits long; and,
  - The only differences between the new Certificate and existing Certificate are one of the following:
    - A new `subjectPublicKey` within the `subjectPublicKeyInfo`, using the same algorithm and key size; and/or,
    - A new `serialNumber`, of the same encoded length as the existing Certificate; and/or
    - The new Certificate's `extKeyUsage` extension is present, has at least one key usage specified, and none of the key usages specified are the id-kp-serverAuth (OID: 1.3.6.1.5.5.7.3.1) or the anyExtendedKeyUsage (OID: 2.5.29.37.0) key usages; and/or
    - The new Certificate's `basicConstraints` extension has a pathLenConstraint that is zero.
- If used within an OCSP response, such as the `signatureAlgorithm` of a BasicOCSPResponse:
  - All unexpired, un-revoked Certificates that contain the Public Key of the CA Key Pair and that have the same Subject Name SHALL also contain an extKeyUsage extension with the only key usage present being the id-kp-ocspSigning (OID: 1.3.6.1.5.5.7.3.9) keyPurposeId.
- If used within a CRL, such as the `signatureAlgorithm` field of a CertificateList or the `signature` field of a TBSCertList:
  - The CRL is referenced by one or more Root CA or Subordinate CA Certificates; and,
  - The Root CA or Subordinate CA Certificate has issued one or more Certificates using this particular encoding for the signature algorithm.

7.1.3.2.2 ECDSA

HARICA SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

- If the signing key is `P-256`, the signature SHALL use ECDSA with SHA-256. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040302`.
- If the signing key is `P-384`, the signature SHALL use ECDSA with SHA-384. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040303`.
- If the signing key is `P-521`, the signature SHALL use ECDSA with SHA-512. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040304`.

7.1.3.2.3 EdDSA

HARICA SHALL indicate an EdDSA key using one of the following algorithm identifiers below:

- For `curve25519` keys, the algorithm SHALL be `id-Ed25519` (OID: 1.3.101.112).
- For `curve448 keys`, the algorithm SHALL be `id-Ed448` (OID: 1.3.101.113).

The parameters for EdDSA keys SHALL be absent. When encoded, the `AlgorithmIdentifier` for EdDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For `Curve25519` keys, `300506032b6570`.
- For `Curve448` keys, `300506032b6571`.

7.1.3.2.4 ML-DSA

HARICA SHALL indicate an ML-DSA key using one of the following algorithm identifiers below:

- `ML-DSA-44` (OID: 2.16.840.1.101.3.4.3.17), or
- `ML-DSA-65` (OID: 2.16.840.1.101.3.4.3.18), or
- `ML-DSA-87` (OID: 2.16.840.1.101.3.4.3.19).

The parameters for ML-DSA keys SHALL be absent. HARICA MUST NOT use HashML-DSA; only “pure” ML-DSA is permitted.
When encoded, the `AlgorithmIdentifier` for ML-DSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For `ML-DSA-44`, `300b0609608648016503040311`.
- For `ML-DSA-65`, `300b0609608648016503040312`.
- For `ML-DSA-87`, `300b0609608648016503040313`.

7.1.3.2.5 ML-KEM

HARICA SHALL indicate an ML-KEM key using one of the following algorithm

identifiers below:

- ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or
- ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
- ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3).

The parameters for ML-KEM keys SHALL be absent.
When encoded, the `AlgorithmIdentifier` for ML-KEM keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For `ML-KEM-512`, `300b060960864801650304040`1.
- For `ML-KEM-768`, `300b060960864801650304040`2.
- For `ML-KEM-1024`, `300b060960864801650304040`3.

7.1.4 Name Forms

7.1.4.1 Serial number

A unique and system generated number SHALL be assigned to each certificate. Duplicate serial numbers are not allowed under the same Issuing CA. Issuing CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least sixty-four (64) bits of entropy from a CSPRNG.

7.1.4.2 Signature Algorithm

The algorithm used to sign the certificate. Limitations are described in section 7.1.3.

7.1.4.3 Signature

The signature of the Certification Authority issuing the certificate. The algorithm used to create the signature is defined in the certificate as described in section 7.1.3.

7.1.4.4 Issuer

The issuer information contains the following fields:

- commonName (OID: 2.5.4.3) (Required): This is the Issuer's Common Name. The contents SHOULD be an identifier for the CA certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- organizationalUnitName (OID: 2.5.4.11) (Optional): Subject Organizational Unit or sub-unit, or special attribute of the signatory depending on the intended use or attributes of the certificate. HARICA prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless HARICA has verified this information in accordance with section 3.2 and the Certificate also contains subject:organizationName and subject:countryName attributes, also verified in accordance with section 3.2.2.1.
- organizationIdentifier (OID: 2.5.4.97) (Required for CAs issuing Qualified Certificates): Per QCP-l and QCP-l-qscd, contains a unique identifier for the Organization per ETSI EN 319 412-3. Depending on the Legal Entity's decision, one of the following identifiers must be used:

  - Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**GR-123456789". In this example, GR is the Subject's Country.
  - Legal Entity's Tax Identification Number with the following semantics: "**VAT**EL-123456789"[6].
- organizationName (OID: 2.5.4.10) (Required): This field SHALL contain either the Subject CA's name or DBA as verified under section 3.2.2.2. If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses. HARICA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that HARICA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", HARICA MAY use "Company Name Inc." or "Company Name".
- localityName (OID: 2.5.4.7) (Optional): Subject Locality as verified under section 3.2.2.1
- stateOrProvinceName (OID: 2.5.4.8) (Optional): Subject State as verified under section 3.2.2.1
- countryName (OID: 2.5.4.6) (Required): Subject Country as verified under section 3.2.2.1

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

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 SHALL be 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 SHALL be 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.

7.1.4.5 Valid From

The date on which the Certificate validity period begins (Format: DD/MM/YYYY HH:MM A.M/P.M GMT).

7.1.4.6 Valid To

The date on which the Certificate validity period ends (Format: DD/MM/YYYY HH:MM A.M/P.M GMT).

7.1.4.7 Subject Information

The subject field identifies the entity associated with the Public Key stored in the subject Public Key field. It contains the following:

- Email (E) (Not applicable for SSL/TLS certificates): The email address of the subject as verified under section 3.2.3.

- commonName (OID: 2.5.4.3) (Optional for SSL certificates, Required for Code Signing and Client Certificates): This is the Subject's Common Name. If present for SSL/TLS certificates, this field SHALL contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension. The value of the field SHALL be encoded as follows:
    - If the value is an IPv4 address, then the value SHALL be encoded as an IPv4Address as specified in RFC 3986, section 3.2.2.
    - If the value is an IPv6 address, then the value SHALL be encoded in the text representation specified in RFC 5952, section 4.
    - For Server TLS Certificates, if the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value SHALL 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 SHALL NOT be converted to their Unicode representation.

- givenName (OID: 2.5.4.42) and/or surname (OID: 2.5.4.4): Per QCP-n and QCP-n-qscd, contain a representation of the Subject's given name and surname as verified under section 3.2.2.1. Further specifications from ETSI EN 319 412-2 apply.
- streetAddress (OID: 2.5.4.9): The physical address of the Subject as verified under section 3.2.2.1.
- postalCode (OID: 2.5.4.17): The postal code for the physical address of the Subject as verified under section 3.2.2.1.
- organizationalUnitName (OID: 2.5.4.11) (Optional): Subject Organizational Unit or sub-unit, or special attribute of the signatory depending on the intended use or attributes of the certificate. HARICA prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless HARICA has verified this information in accordance with section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with section 3.2.2.1. This field SHALL NOT be present in SSL/TLS Certificates.
- organizationName (OID: 2.5.4.10): This field SHALL contain the Subject's name as verified under section 3.2.2.1 and/or DBA/tradename as verified under section 3.2.2.2. If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses. HARICA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that HARICA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", HARICA MAY use "Company Name Inc." or "Company Name". For TLS OV/EV Certificates, this field is required and it is optional for TLS IV Certificates if the Natural Person's subject information is included in the givenName and surname fields, and the information is verified under section 3.2.3. For EV Certificates, this attribute must be verified according to section 7.1.4.2.1 of the EV Guidelines.

- localityName (OID: 2.5.4.7) (Optional): The city, village or local territory where the subject entity is located, as verified under section 3.2.2.1. For TLS OV/EV Certificates it is required if stateOrProvinceName is missing, otherwise it is optional.
- stateOrProvinceName (OID: 2.5.4.8) (Optional): The state, prefecture or wider geographical division where the subject entity is located, as verified under section 3.2.2.1. For TLS OV/EV Certificates it is required if localityName is missing, otherwise it is optional.
- countryName (OID: 2.5.4.6): Subject Country as verified under section 3.2.2.3
- Subject Public Key Information: Contains the Public Key and identifies the algorithm with which the Key is used and its size. Code Signing certificates SHALL chain up to a 4096-bit RSA or ECC equivalent (P384) CA.
- serialNumber (OID: 2.5.4.5) (Required for EV, QEVCP-w, QCP-n, QCP-n-qscd)(Optional for LCP, NCP, NCP+, QNCP-w, QNCP-w-gen):
    - Per EV and QEVCP-w it contains the Registration Number of the Legal Entity of the Subject.
        - For Private Organizations, this field SHALL contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.

        - For Government Entities that do not have a Registration Number or readily verifiable date of creation, HARICA SHALL enter the value “Government Entity”.

        - For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.

    - Per QCP-n and QCP-n-qscd, contains a unique identifier to disambiguate the Subject Name within the context of an Issuing CA per ETSI EN 319 412-2. Depending on the Person’s decision, one of the following identifiers may be used:
        - National personal number (or national civic registration number with the following semantics: “**PNO**GR-12345678”. In this example, GR is the Subject’s Country.
        - National identity card number with the following semantics: “**IDC**GR-AK1234567”. In this example, GR is the Subject’s Country.

  - Tax Identification Number according to the European Commission - Tax and Customs Union (https://ec.europa.eu/taxation_customs/tin/tinByCountry.html) with the following semantics: "**TIN**EL-123456789"[6]. HARICA also allows the use of TINGR-123456789.
  - Passport Number with the following semantics: "**PAS**GR-1231232". In this example, GR is the Subject's Country.
  - A Unique 10-digit Identifier assigned by HARICA
- businessCategory (OID: 2.5.4.15): For EV Certificates, this attribute must contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of section 4.1.1.1, 4.1.1.2, 4.1.1.3 or 4.1.1.4 of the EV Guidelines, respectively.
- *jurisdictionCountryName* (OID: 1.3.6.1.4.1.311.60.2.1.3), *jurisdictionStateOrProvinceName* (OID: 1.3.6.1.4.1.311.60.2.1.2), *jurisdictionLocalityName* (OID: 1.3.6.1.4.1.311.60.2.1.1): For EV Certificates, this is the Subject Jurisdiction of Incorporation or Registration Field according to section 7.1.4.2.4 of the EV Guidelines.
- OrganizationIdentifier (OID: 2.5.4.97): Per QCP-l, QCP-l-qscd, QNCP-w-OV, QNCP-w-gen (for Legal Entities) this attribute shall contain a Registration Reference for the Organization per ETSI EN 319 412-3. The Registration Reference SHOULD be unique where the Registration Scheme and jurisdiction provide unique identifiers. Depending on the Legal Entity's decision, one of the following identifiers must be used:
  - Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**GR-123456789". In this specific example, GR is the Subject's Country.
  - Legal Entity's Tax Identification Number with the following semantics: "**VAT**EL-123456789"[6]. HARICA also allows the use of VATGR-123456789.
  - Legal Entity's Legal Entity Identifier with the following semantics: "**LEIXG**-123456789"[7] validated as specified in section 3.2.2.1.1.

  Per EVCP or QEVCP-w this attribute shall contain a unique identifier for the Organization according to section 7.1.4.2.8 of the EV Guidelines.

  For OV and SV S/MIME certificates this attribute shall contain a unique identifier for the Organization according to section 7.1.4.2.2 of the Baseline Requirements for S/MIME Certificates.

[6] It is noted that in accordance with the National Supervisory Body, it is strongly recommended to use the value "EL" instead of "GR" when the prefix is "TIN" or "VAT".

[7] "LEI" is the prefix to indicate a global Legal Entity Identifier as specified in ISO 17442. According to ETSI EN 319 412-1, when LEI is used, the 2-character ISO 3166-1 country code shall be set to "XG".

For PSD2 Certificates, the semantics shall follow clause 5.1.4 of ETSI EN 319 412-1 which uses the scheme **"PSD"** for identification based on national authorization number of a payment service provider under Payments Services Directive (EU) 2015/2366. This shall use the extended structure as defined in ETSI TS 119 495, clause 5.2.1.
For the NTR Registration Scheme, when the Organization or Legal Entity is registered in the European Union or the European Economic Area, the Registration Reference MAY use the EUID identifier. When the Organization or Legal Entity is registered in Germany, the Registration Reference SHOULD use the EUID identifier. The structure of the EUID SHALL be as follows:

- 2 character ISO 3166-1 country code, which must match the country code used in the leading string 'NTR'; and
- the business register identifier for the particular section or office of the domestic register that assigned the Registration Reference; and
- dot-sign '.' (U+002E); and
- the Registration Reference allocated by the domestic register.

For example:

- NTRDE-DER3306.HRB12345 (DE is the country code for Germany, R3306 is the business register identifier for the district court in Cologne, and HRB12345 is the locally-assigned Registration Reference).

- With the exception of EV Certificates, other subjectDN attributes MAY be present within the subject field. If present, other attributes SHALL contain information that has been verified by HARICA.

By issuing an SSL/TLS Certificate, HARICA represents that it followed the procedures set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all Subject Information was accurate. HARICA shall not include a Domain Name or IP Address in a Subject attribute except as specified in section 3.2.2.4 or section 3.2.2.5. Subject attributes for SSL/TLS Certificates SHALL NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

By issuing a Client/CodeSigning Certificate, HARICA represents that it followed the procedures set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all Subject Information was accurate. HARICA shall not include a commonName, emailAddress in a Subject attribute except as specified in section 3.2.3. Because Subject name attributes for individuals (e.g. givenName (OID: 2.5.4.42) and surname (OID: 2.5.4.4)) are not broadly supported by application software, HARICA may use the subject:organizationName field to convey a natural person Subject's name or DBA. Subscribers are bound to provide complete, accurate and truthful information (e.g., application name, information URL, application description, etc.) in the signed code. Subscribers are also committed to not deliberately sign Suspect Code and acknowledge that such an action will allow HARICA to automatically revoke the signing Certificate.

By issuing a Certificate for Advanced electronic signatures under the QCP-n policy or a Certificate for Qualified electronic signatures under the QCP-n-qscd policy, HARICA shall include at least the “commonName”, “Country”, “givenName” and “surname” attributes in the SubjectDN field. If these attributes are not sufficient to ensure Subject name uniqueness within the context of the Issuing CA, then the serialNumber shall be present.

By issuing a Certificate for Advanced electronic seals under the QCP-l policy or a Certificate for Qualified electronic seals under the QCP-l-qscd policy, HARICA shall include at least the “commonName”, “Country”, "organizationName" and "OrganizationIdentifier” attributes in the SubjectDN field.

For server authentication TLS Certificates, when encoding a Name, HARICA SHALL ensure 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 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates.
- 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.
- For attributes in the Certificate subject field that are listed in the table “Encoding and Order Requirements for Selected Attributes of Section 7.1.4.2 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificate, HARICA SHALL follow the specified encoding requirements for each attribute.

7.1.5 Name constraints

HARICA may use the name constraints extension per RFC 5280, in order to limit the scope of Subordinate CAs. This extension is marked as “non-critical”.

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate SHALL include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for. The `anyExtendedKeyUsage` KeyPurposeId SHALL NOT appear within this extension.

If a Subordinate CA Certificate includes the `id-kp-serverAuth` KeyPurposeId in the extended key usage extension and the respective Subordinate CA needs to be treated as technically constrained for SSL/TLS Server Certificates and audited as described in

section 8.7, then the Subordinate CA Certificate SHALL include the Name Constraints X.509v3 extension with constraints on `dNSName, iPAddress` and `DirectoryName` as follows:

a) For each dNSName in permittedSubtrees, HARICA SHALL confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of section 3.2.2.4.
b) For each iPAddress range in permittedSubtrees, HARICA SHALL confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.
c) For each DirectoryName in permittedSubtrees HARICA SHALL confirm the Applicants and/or Subsidiary's Organizational name and location such that end entity certificates issued from the subordinate CA Certificate will be in compliancy with section 7.1.2

If the Subordinate CA Certificate includes the id-kp-serverAuth KeyPurposeId in the extended key usage extension and the respective Subordinate CA needs to be treated as technically constrained for SSL/TLS Server Certificates and audited as described in section 8.7 and not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate SHALL specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate SHALL include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate SHALL also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate SHALL include at least one iPAddress in permittedSubtrees.

If the Subordinate CA Certificate includes an extended key usage other than the `id-kp-serverAuth` [RFC5280] or `anyExtendedKeyUsage` [RFC5280] it is treated as technically constrained for SSL/TLS Server Certificates and audited as described in section 8.7.

7.1.6 Certificate policy object identifier

The OID (Object Identifier) of this certificate policy is stated in section 1.2. According to each certificate type, the following recognized OIDs can be added in the *certificatePolicies* extension:

- **BTSP** (Best practice policy for time-stamp)
  - **0.4.0.2023.1.1** as specified in ETSI EN 319 421
  - 1.3.6.1.4.1.26513.1.1.6.1
- **QTST** (Qualified time-stamping Certificate)
  - **0.4.0.2023.1.1** as specified in ETSI EN 319 421
  - 1.3.6.1.4.1.26513.1.1.6.2
- **Time-stamping for Code Signing**
  - **2.23.140.1.4.2** as described in CA/B Forum Baseline Requirements for Code Signing
  - 1.3.6.1.4.1.26513.1.1.6.3
- **QCP-n** (Advanced Electronic Signature)

    - **0.4.0.194112.1.0** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.1
- **QCP-l** (Advanced Electronic Seal)
    - **0.4.0.194112.1.1** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.3
- **QCP-l-psd2** (Advanced Electronic Seal for PSD2)
    - **0.4.0.194112.1.1** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.5
- **QCP-l-psd2-qscd** (Qualified Electronic Seal for PSD2)
    - **0.4.0.194112.1.3** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.6
- **QCP-n-qscd** (Qualified Electronic Signature)
    - **0.4.0.194112.1.2** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.2
- **QCP-l-qscd** (Qualified Electronic Seal)
    - **0.4.0.194112.1.3** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.4
- **QEVCP-w** (Qualified Website Authentication Certificate for Legal Entity)
    - **0.4.0.194112.1.4** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.1.5
- **QNCP-w-OV** (Qualified Website Authentication Certificate for Legal Entity)
    - **0.4.0.194112.1.5** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.1.7
- **QNCP-w-IV** (Qualified Website Authentication Certificate for Natural Person)
    - **0.4.0.194112.1.5** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.1.8
- **QNCP-w-gen** (Qualified Website Authentication Certificate for Legal Entity)
    - **0.4.0.194112.1.6** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.1.9
- **QEVCP-w-psd2** (Qualified Website Authentication Certificate for PSD2)
    - **0.4.0.19495.3.1** as described in ETSI TS 119 495
    - 1.3.6.1.4.1.26513.1.1.1.6
- **NCP** (Normalized Certificate Policy)
    - **0.4.0.2042.1.1** as described in ETSI EN 319 411-1
    - 1.3.6.1.4.1.26513.1.1.2.2.1
    - 1.3.6.1.4.1.26513.1.1.2.2.4
    - 1.3.6.1.4.1.26513.1.1.2.2.5
    - 1.3.6.1.4.1.26513.1.1.2.4.4
    - 1.3.6.1.4.1.26513.1.1.2.4.5
    - 1.3.6.1.4.1.26513.1.1.2.4.6
    - 1.3.6.1.4.1.26513.1.1.2.3.1
    - 1.3.6.1.4.1.26513.1.1.3.1.1
    - 1.3.6.1.4.1.26513.1.1.3.2.1
    - 1.3.6.1.4.1.26513.1.1.5.1.1
    - 1.3.6.1.4.1.26513.1.1.5.2.1
- **NCP+** (Extended Normalized Certificate Policy)
    - **0.4.0.2042.1.2** as described in ETSI EN 319 411-1
    - 1.3.6.1.4.1.26513.1.1.2.2.2

    - 1.3.6.1.4.1.26513.1.1.2.3.2
    - 1.3.6.1.4.1.26513.1.1.3.1.2
    - 1.3.6.1.4.1.26513.1.1.3.2.2
    - 1.3.6.1.4.1.26513.1.1.5.1.2
    - 1.3.6.1.4.1.26513.1.1.5.2.2
- **LCP** (Lightweight Certificate Policy)
    - **0.4.0.2042.1.3** as described in ETSI EN 319 411-1
    - 1.3.6.1.4.1.26513.1.1.2.1.1
    - 1.3.6.1.4.1.26513.1.1.2.1.2
    - 1.3.6.1.4.1.26513.1.1.2.1.3
    - 1.3.6.1.4.1.26513.1.1.2.4.1
    - 1.3.6.1.4.1.26513.1.1.2.4.2
    - 1.3.6.1.4.1.26513.1.1.2.4.3
    - 1.3.6.1.4.1.26513.1.1.2.2.3
    - 1.3.6.1.4.1.26513.1.1.2.3.3
    - 1.3.6.1.4.1.26513.1.1.5.1.3
    - 1.3.6.1.4.1.26513.1.1.5.2.3
- **DVCP** (Domain Validated Certificate Policy)
    - **0.4.0.2042.1.6** as described in ETSI EN 319 411-1
    - **2.23.140.1.2.1** as described in CA/B Forum Baseline Requirements
    - 1.3.6.1.4.1.26513.1.1.1.1
- **OVCP** (Organizational Validation Certificate Policy)
    - **0.4.0.2042.1.7** as described in ETSI EN 319 411-1
    - **2.23.140.1.2.2** as described in CA/B Forum Baseline Requirements
    - 1.3.6.1.4.1.26513.1.1.1.2
- **IVCP** (Individual Validation Certificate Policy)
    - **0.4.0.2042.1.8** as described in ETSI EN 319 411-1
    - **2.23.140.1.2.3** as described in CA/B Forum Baseline Requirements
    - 1.3.6.1.4.1.26513.1.1.1.3
- **EVCP** (Extended Validation Certificate Policy)
    - **0.4.0.2042.1.4** as described in ETSI EN 319 411-1
    - **2.23.140.1.1** as described in CA/B Forum EV Guidelines
    - 1.3.6.1.4.1.26513.1.1.1.4
- **Non-EV Code Signing**
    - **2.23.140.1.4.1** as described in CA/B Forum Baseline Requirements for Code Signing for Non-EV Code Signing Certificates
    - 1.3.6.1.4.1.26513.1.1.3.1.1
    - 1.3.6.1.4.1.26513.1.1.3.1.2
    - 1.3.6.1.4.1.26513.1.1.3.2.1
    - 1.3.6.1.4.1.26513.1.1.3.2.2
- **EV** (Extended Validation) **for Code Signing**
    - **2.23.140.1.3** as described in CA/B Forum EV Guidelines for Code Signing.
    - 1.3.6.1.4.1.26513.1.1.3.3
- **OCSP Certificate**
    - 1.3.6.1.4.1.26513.1.1.7
- **Remote QSCD**
    - 1.3.6.1.4.1.26513.1.1.8

A complete list of Policy OIDs is available in ANNEX F HARICA .

Internally Operated Subordinate CAs can use the reserved “AnyPolicy” OID **2.5.29.32.0**. In the case of Externally Operated Subordinate CAs, the corresponding CP/CPS OID must be used in the Subordinate CA Certificate Policy Extension.

If a Subordinate CA Certificate is enabled to issue Qualified Certificates and does not include the `subject:organizationIdentifier` field, then the certificatePolicies extension shall include a userNotice with the value: “*This Qualified Certificate has been Issued by the QTSP "Greek Universities Network (GUnet)" with VAT number EL099028220*”.

Subscriber SSL/TLS Certificates SHALL contain one of the CA/Browser Forum reserved policy OIDs in the `certificatePolicies` extension.

Effective July 15, 2025 S/MIME Subscriber Certificates SHALL NOT be issued using the CA/Browser Forum Legacy Generation profiles 2.23.140.1.5.1.1, 2.23.140.1.5.2.1, 2.23.140.1.5.3.1, or 2.23.140.1.5.4.1.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

If the policy qualifier `cPSuri` [RFC 5280] is used, it SHALL point to the URI of the published HARICA CP/CPS documents.

If the policy qualifier `userNotice` [RFC 5280] is used, it shall include a text to convey specific policy information or information related to the Trust Service Provider.
For Qualified Certificates the following text MAY be used to include more information about HARICA acting as a Trust Service Provider Issuing the Qualified Certificate:
“This Qualified Certificate has been Issued by the QTSP "Greek Universities Network (GUnet)" with VAT number EL099028220”.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

7.2.1 Version number(s)

The version number is 2 (the integer value is 1), which corresponds to CRL X.509v2, per RFC 5280.

7.2.2 CRL and CRL entry extensions

7.2.2.1 Signature

The signature algorithm SHALL follow the requirements described in sections 6.1.5 and 6.1.6.

7.2.2.2 Hashing Algorithm

The hashing algorithm SHALL use a hashing algorithm from the SHA2 family or stronger

7.2.2.3 Issuer Name

The Distinguished Name of the Certification Authority that has signed and issued the CRL, byte-for-byte.

7.2.2.4 This Update

Issue date of the CRL in UTCTime.

7.2.2.5 Next Update

Date by which the next CRL shall be issued in UTCTime. The requirements of section 4.9.7 apply.

If a Subordinate CA:

1. has issued Certificates that are either expired or revoked and
2. stops issuing new Certificates

then this Subordinate CA may generate the last CRL and may set the `nextUpdate` field in the CRL defined in RFC 5280 to "`99991231235959Z`". This value, defined in RFC 5280 for certificates that have no well-defined expiration date, is here extended for CRL. The Issuing CA that generates a last CRL SHALL NOT issue any new Certificates.

7.2.2.6 Revoked Certificates

List of all revoked certificates including their serial number and the date and time of the revocation in UTCTime.

7.2.2.7 CRL Number (OID 2.5.29.20)

This extension SHALL be included and SHALL NOT be marked critical. It contains a sequentially increasing unique number identifying each CRL per section 5.2.3 of RFC 5280.

7.2.2.8 Authority Key Identifier

This extension SHALL be included and SHALL NOT be marked critical. It contains the authority key identifier of the Issuing CA as described in section 5.2.1 of RFC 5280.

7.2.2.9 expiredCertsOnCRL (OID: 2.5.29.60)

This extension MAY be present and SHALL NOT be marked critical. It indicates that the CRL includes revocation notices for expired certificates as described in section 9.5.2.8 of ITU-T X.509.

7.2.2.10 reasonCode (OID 2.5.29.21)

If present, this CRL entry extension SHALL NOT be marked critical.

For CAs technically capable of issuing SSL/TLS Certificates, if a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension SHALL be present.

If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements:

- The `CRLReason` indicated SHALL NOT be unspecified (0). If the reason for revocation is unspecified, Issuing CAs SHALL omit `reasonCode` entry extension, if allowed by the previous requirements. If a CRL entry is for a SSL/TLS Certificate, the `CRLReason` SHALL NOT be certificateHold (6). See section 4.9.15 for more information.
- If a `reasonCode` CRL entry extension is present, the `CRLReason` SHALL indicate the most appropriate reason for revocation of the certificate based on section 4.9.1.
- `CRLReason` SHALL be included in the `reasonCode` extension of the CRL entry corresponding to a SSL/TLS Subscriber Certificate, unless the `CRLReason` is "unspecified (0)".

According to section 9.5.3.1 of the ITU-T X.509 recommendation and RFC 5280, only specific reason codes are allowed in the `CRLReason` field of the `reasonCode` extension of each CRL entry. Only the following `CRLReasons` MAY be present in the CRL `reasonCode` extension for Subscriber Certificates:

- **keyCompromise (RFC 5280 CRLReason #1)**: Indicates that it is known or suspected that the Subscriber's Private Key has been compromised;
- **affiliationChanged (RFC 5280 CRLReason #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 (RFC 5280 CRLReason #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 (RFC 5280 CRLReason #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; or
- **privilegeWithdrawn (RFC 5280 CRLReason #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.
- **certificateHold (RFC 5280 CRLReason #6):** It is intended when a Public-Key Certificate is placed on hold (i.e. suspended). See sections 4.9.15 for more information. This reason is not allowed to be used for SSL/TLS or Code Signing Subscriber Certificates.

7.2.2.11 issuingDistributionPoint (OID 2.5.29.28)

If present, this CRL entry extension SHALL NOT be marked critical.

If a CRL does not contain entries for all revoked unexpired certificates issued by the CRL issuer, then it SHALL contain a critical Issuing Distribution Point extension and SHALL populate the `distributionPoint` field of that extension.

Partitioned CRLs MUST contain an Issuing Distribution Point extension. The `distributionPoint` field of the Issuing Distribution Point extension MUST be present. Additionally, the `fullName` field of the DistributionPointName value MUST be present, and its value MUST conform to the following requirements:

1. If a Certificate within the scope of the CRL contains a CRL Distribution Points extension, then at least one of the `uniformResourceIdentifiers` in the CRL Distribution Points's `fullName` field MUST be included in the `fullName` field of the CRL's Issuing Distribution Point extension. The encoding of the `uniformResourceIdentifier` value in the Issuing Distribution Point extension SHALL be byte-for-byte identical to the encoding used in the Certificate's CRL Distribution Points extension.

2. Other GeneralNames of type `uniformResourceIdentifier` MAY be included.

3. Non-`uniformResourceIdentifier` GeneralName types MUST NOT be included.

The `indirectCRL` and `onlyContainsAttributeCerts` fields MUST be set to `FALSE` (i.e., not asserted).

HARICA MAY set either of the `onlyContainsUserCerts` and `onlyContainsCACerts` fields to `TRUE`, depending on the scope of the CRL.

HARICA MUST NOT assert both of the `onlyContainsUserCerts` and `onlyContainsCACerts` fields.

The `onlySomeReasons` field SHOULD NOT be included; if included, then HARICA MUST provide another CRL whose scope encompasses all revocations regardless of reason code.

This extension is NOT RECOMMENDED for full and complete CRLs.

7.3 OCSP Profile

The OCSP responders SHALL conform to RFC 6960.

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the `revocationReason` field within the `RevokedInfo` of the `CertStatus` SHALL be present.

The `CRLReason` indicated SHALL contain a value permitted for CRLs, as specified in section 7.2.2.

7.3.1 Version number

Version 1 of the OCSP specification as defined by RFC 6960 is supported.

7.3.2 OCSP extensions

The OCSP service uses a secure timestamp and a maximum validity period as defined in section 4.9.10 to verify the freshness of the signed response. The next updates are available at least one day before the current period expires. The hash algorithm used for signing the OCSP responses is SHA2.

The `singleExtensions` of an OCSP response SHALL NOT contain the `reasonCode` (OID 2.5.29.21) CRL entry extension but MAY contain the `ArchiveCutOff` (OID 1.3.6.1.5.5.7.48.1.6) per section 4.4.4 of RFC 6960.

8 Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

CA Certificates that are capable of being used to issue new certificates SHALL either be Technically Constrained in line with section 7.1.5 and audited in line with section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section.

An external CP/CPS compliance audit is required on a yearly basis. The period during which HARICA issues Certificates SHALL be divided into an unbroken sequence of audit periods.

The audit period for a Delegated Third Party SHALL NOT exceed the audit period of HARICA's compliance audit.

8.2 Identity/qualifications of assessor

HARICA's external audit is performed by a Qualified and accredited Auditor, according to the specifications of the audit criteria.

8.3 Assessor's relationship to assessed entity

External auditors must be independent from any relationships that might constitute a conflict of interest, or that could in any way impair the external auditor's objective assessment.

8.4 Topics covered by assessment

HARICA PKI meets the specifications of:

- ETSI EN 319 411-1 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing certificates; Part 1: General Requirements*",

- ETSI EN 319 411-2 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*",
- ETSI TS 119 411-6 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing certificates Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificate.*",
- ETSI EN 319 421 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing Time-Stamps*", and
- Regulation (EU) No 910/2014 (eIDAS) of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market as amended by Regulation (EU) 1183/2024.

HARICA has also included guidelines and procedures from the following documents:

- "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates",
- "Guidelines for the Issuance and Management of Extended Validation Certificates,
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates",
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Code Signing Certificates", and
- "Network and Certificate System Security Requirements".

published at https://www.cabforum.org.

In addition to the above standards, HARICA complies with

- ETSI TS 119 495 that supports Qualified Certificate Profiles and TSP Policy Requirements for Open Banking, which includes the payment services Directive (EU) 2015/2366, the Delegated Regulation (EU) 2018/389 with regard to Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication, and
- the Ministerial Decision 27499/2021-08 for Remote Identity Proofing.

For Delegated Third Parties which are not Enterprise RAs, HARICA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in this, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or HARICA's CP/CPS.

If the opinion of the auditor is that the Delegated Third Party does not comply, then HARICA SHALL not allow the Delegated Third Party to continue performing delegated functions until the proper remediations are applied and the Delegated Third Party returns to a fully-compliant state.

For Audit Periods beginning on or after **March 15, 2025**, CA private keys that have been generated but not yet associated with a CA certificate ("parked keys") MUST be identified by the SHA-256 hashes of the CA Public Keys. Specifically, the SHA-256 hash MUST be calculated over the DER encoding of the `SubjectPublicKeyInfo`

containing the CA Public Key and included in auditor-provided annual key lifecycle management reports (or a corresponding section or appendix of HARICA's audit reports). These reports must account for the controls and measures applied to ensure the integrity, confidentiality, and protection of these keys throughout their lifecycle, consistent with the audit criteria cited above.

8.5 Actions taken because of deficiency

If a Subordinate CA is shown to be non-conformant in any way to the warranties listed in section 9.6.1.1, and fails to significantly meet their objectives, it shall cease issuing certificates using the corresponding policy identifier until it has been assessed as conformant.

8.6 Communication of results

The Audit Report states explicitly the scope of the audit criteria. The most recent audit report will be publicly available on the main web site of HARICA (https://www.harica.gr). These reports will also be submitted to Application Software Suppliers for the various Root CA Programs and the National supervisory body. HARICA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. Certain Application Software Suppliers require special template forms to be filled in and signed by the auditors. These forms are not required to be made publicly available but are submitted directly to the corresponding Application Software Supplier.

Each Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.

In addition, audit attestation letters associated with Publicly-Trusted Certificates SHALL be uploaded to the CCADB within ninety (90) calendar days from the audit period ending date specified in the audit attestation letter. An authoritative English language version of the publicly available audit attestation letter SHALL be provided by the Qualified Auditor and HARICA SHALL ensure it is publicly available.

8.7 Self-Audits

HARICA, at all times, shall monitor adherence to this CP/CPS and 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 (3%) of the Publicly Trusted Certificates issued for SSL/TLS or Code Signing use, including EV Certificates. For all EV Certificates where the Final Cross-Correlation and Due Diligence requirements of section 3.2.13 of the EV Guidelines is performed by an external RA, HARICA SHALL strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent (6%) of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

During the period in which a Technically Constrained Subordinate CA issues Certificates for SSL/TLS use, HARICA SHALL monitor adherence to this CP/CPS.

Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4, if HARICA uses a Delegated Third Party entity to participate in the validation process for the issuance of TLS or Code Signing Certificates, HARICA SHALL contractually obligate each Delegated Third Party, Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in this CP/CPS, EV Guidelines and to perform them as required of HARICA itself. HARICA SHALL enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with the EV Guidelines on an annual basis. HARICA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party complies with this CP/CPS. HARICA SHALL internally audit each Delegated Third Party's compliance with this CP/CPS at the same frequency as HARICA's compliance audit.

HARICA SHALL complete and submit an annual self-assessment to the CCADB covering requirements of at least the following:

- CCADB Policy
- Chrome Root Program Policy
- Mozilla Root Store Policy
- Network and Certificate System Security Requirements
- Baseline Requirements for Publicly-Trusted TLS Certificates
- Extended Validation Guidelines for Publicly-Trusted TLS Certificates

9 Other Business and Legal Matters

9.1 Fees

No dues are paid for the provided services for Hellenic Academic and Research Institutions. HARICA reserves the right to charge fees for Subscribers outside the main constituency. Exploitation or subcontracting of provided services from organizations affiliated with HARICA is expressly prohibited.

9.1.1 Certificate issuance or renewal fees

HARICA reserves the right to charge fees for Subscribers outside the main constituency.

9.1.2 Certificate access fees

No fees are charged for individual certificate access.

9.1.3 Revocation or status information access fees

No fees are charged for revocation or status information access.

9.1.4 Fees for other services

HARICA reserves the right to charge fees for services outside the standard certificate lifecycle process.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

HARICA bears no responsibility and therefore shall not undertake or pay damages for potential liability, unless specified otherwise in the current CP/CPS.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Private keys of the Certification Authorities, the source code and the private keys for storage/operation procedures are considered classified and confidential information. Information concerning the physical access and security of the premises where the Certification and Registration Authorities are installed and operated, is also considered classified.

The Business Continuity plan and disaster recovery plans are also kept confidential.

9.3.2 Information not within the scope of confidential information

Information included in the issued digital certificates and revocation data is not considered confidential.

9.3.3 Responsibility to protect confidential information

HARICA staff and contractors are responsible for protecting confidential information, not to use such data for other unintended purpose and are explicitly and contractually bound to do so. HARICA staff and operators are trained on how to use and handle confidential information as mentioned in section 5.3. HARICA takes all appropriate technical and organizational measures to enforce this policy.

9.4 Privacy of personal information

9.4.1 Privacy plan

HARICA has implemented a Data Protection Policy and issued its Data Privacy Statement, available at https://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf in compliance with applicable laws relating to data protection and any equivalent legislation and EU Regulations.

9.4.2 Information treated as private

Registration Authorities undergo personal information processing during the identification and validation procedure of the Applicant which is treated as private. Personal information is not disclosed unless it is required by law or included in the certificate public information (for example the *subject* field of the certificate) with Applicant's consent. If the Applicant agrees to include personal information related to personal identification described in 7.1.4.7 (Social Security Number, Personal Identification, Tax Identification, Passport Number) in the Subscriber Certificate, then this information is not considered private.

9.4.3 Information not deemed private

Information included in the issued digital certificates is not considered private. If the Applicant, during the Certificate request process, requested personal information to be embedded in the issued Certificate, the Subscriber consents to HARICA's disclosure of this information publicly by embedding the information in the issued Certificate. Subscriber Certificates are publicly disclosed at HARICA's Repository, which implements restrictions to protect against enumeration attacks.

9.4.4 Responsibility to protect private information

All private and personal information handled and processed by HARICA, is in accordance with the Greek legislation concerning personal data protection. There are specific technical and organizational measures in place to prevent unauthorized and unlawful processing or accidental loss of private and personal information.

9.4.5 Notice and consent to use private information

Unless otherwise stated in this CP/CPS, the applicable Data Privacy Statement (available at https://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf) or by agreement, all private and personal information handled and processed by HARICA are not used without prior notice or consent, where applicable, of the data subject to whom it concerns, in accordance with applicable data protection laws and any equivalent legislation and EU Regulations.

9.4.6 Disclosure pursuant to judicial or administrative process

All non-classified information stored at the Certification and Registration Authorities is available to the law enforcement authorities, after their official written request.

Classified and personal information can be disclosed to the judicial authority if a properly constituted and enforceable instrument is issued, such an official court order, judgment or administrative action or demand, in accordance with general principles of law and applicable legislation.

The process is carried out through the Policy Management Committee of HARICA (see section 1.5). Private keys used to sign and issue digital certificates are never disclosed to any third parties, unless HARICA is obliged to such disclosure under applicable and enforceable law.

9.4.7 Other information disclosure circumstances

All non-classified and non-private information stored at the Certification and Registration Authorities is available for entity queries, upon request for reasons of legitimate interest.

All information stored at the CA and RA is available to its rightful owner (e.g. individual who applied for a certificate), upon rightful owner's request.

This section is subject to applicable data protection laws and EU Regulations.

9.4.7.1 Publicity

By accepting the Terms, Subscriber grants HARICA the right to use Subscriber's brand name and/or logo, to identify as a customer on HARICA's website or other marketing or advertising materials without any previous notice.

Subscribers may opt out by informing HARICA at support@harica.gr, within the first 30 days of their subscription.

9.5 Intellectual property rights

HARICA owns the intellectual property rights for its PKI services. It does not hold any intellectual property rights on the keys of Subscriber's issued certificates.

Anyone can copy parts of this CP/CPS with the condition that the original document is properly referenced.

Parts of the CA/B Forum Baseline Requirements, EV Guidelines, Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates, Apple, Google Chrome, Microsoft and Mozilla Root Program Requirements are used in this CP/CPS.

Subscribers shall not use HARICA's trademark without any previous notice and HARICA's written consent.

9.6 Representations and warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, HARICA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier and
3. Relying Parties who reasonably rely on a Valid Certificate.

HARICA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, HARICA has complied with this CP/CPS in issuing and managing the Certificate.

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

- ✓ Provide and maintain the infrastructure that is required for constitution of hierarchy of a Trust Service Provider, according to the certification processes described in this document.
- ✓ Implement and maintain the security requirements according to relative sections of the present document
- ✓ Accept or reject requests for certificate issuance according to the relative sections of the present document.

- ✓ Maintain a publicly accessible directory for certificates and CRLs. This information should be publicly available via widely used protocols such as HTTP, FTP and LDAP.
- ✓ Revoke certificates when specific reasons apply or after a proper request by the subject of the certificate.
- ✓ Maintain the CRLs up to date.
- ✓ Manage all personal and private information of the Subscribers with confidentiality.
- ✓ Without undue delay inform the technical personnel of Subordinate CAs for any loss, exposure, modification or unauthorized usage of the CA's private key.
- ✓ Ensure that all the services provided within the whole infrastructure, abide by the terms and conditions of the present CP/CPS.
- ✓ HARICA maintains a 24 x 7 publicly accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates
- ✓ HARICA will revoke the Certificate for any of the reasons specified in section 4.9.1.1 of this CP/CPS.

For Extended Validation Certificates, the EV Certificate Warranties specifically include, but are not limited to, the following:

1. **Legal Existence:** HARICA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
2. **Identity:** HARICA has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
3. **Right to Use Domain Name:** HARICA has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the right to use all the Domain Name(s) included in the EV Certificate;
4. **Authorization for EV Certificate:** HARICA has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
5. **Accuracy of Information:** HARICA has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
6. **Subscriber Agreement:** The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with HARICA that satisfies the requirements of this CP/CPS or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
7. **Status:** HARICA will follow the procedures of this CP/CPS and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and

8. **Revocation:** HARICA will follow the procedures of this CP/CPS and revoke the EV Certificate for any of the revocation reasons specified in this CP/CPS.

HARICA SHALL be responsible for the performance and warranties of the Subordinate CAs, for the Subordinate CA's compliance with this CP/CPS and for all liabilities and indemnification obligations of the Subordinate CAs under this CP/CPS, as if HARICA were the Subordinate CA issuing the Certificates.

HARICA makes the following warranties for its TSA Subscribers and the produced TSTs:

- ✓ Provide and maintain the time stamping infrastructure that is required for constitution of hierarchy of a Trust Service Provider, per the certification processes described in this document.
- ✓ The TSUs maintain a minimum accuracy of ± 1 second to UTC time
- ✓ Implement and maintain the security requirements according to relative sections of the present document.

9.6.1.1 Responsibilities of externally-operated Certification Authorities

Each externally-operated Certification Authority approved by HARICA is committed to:

- ✓ Follow all rules and procedures that apply to this CP/CPS regarding Certification Authorities.
- ✓ Grant certificates with validity period within the limits of the active employment (or other) relationship between the Applicant and the institution or organization, according to the Applicant's affiliation (i.e. student, employee, and faculty).
- ✓ Inform the parent Certification Authority without undue delay in case of private key exposure.
- ✓ Protect the private keys, used for certificate signing, at least in the security level that is described in the present document.
- ✓ Develop (optionally) its own policies and procedures of certification which must be at least as strict and binding as the ones described in the present document.
- ✓ In case an organization wants to run an externally-operated subCA, according to its certification scope, it SHALL provide a conformity assessment report according to the latest versions of ETSI EN 319 411-1, ETSI EN 319 411-2 (or equivalent) requirements and the latest version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document produced by the CA/Browser Forum (www.cabforum.org).

9.6.2 RA Representations and Warranties

- ✓ Each Registration Authority is responsible to receive certificate applications from Applicants. It validates the identity of the Applicant, confirms that the public key that is submitted belongs to the Applicant and securely transmits the application to the CA.
- ✓ According to the certificate type, applications can be submitted via face-to-face meeting with the interested party, via email, via a secure web form, or via any mechanism that securely identifies the Applicant. The application includes all information identifying the Subscriber, and the corresponding public key.

- ✓ Mass applications submission from a specific department or organization is possible on behalf of the persons that belong to that department or organization
- ✓ Each Registration Authority must verify if each person requesting a personal certificate is the rightful owner of the certified email address.
- ✓ Each Registration Authority must verify that the person requesting a device certificate is the rightful owner and administrator of the device's FQDN.
- ✓ In case an organization wants to run its own RA, according to its certification scope, it SHALL provide a conformity assessment report according to the latest versions of ETSI EN 319 411-1, ETSI EN 319 411-2 (or equivalent) requirements and the latest version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document produced by the CA/Browser Forum (www.cabforum.org).

RAs are also committed to secure the following:

- ✓ **Right to Use Domain Name:** That, at the time of issuance, HARICA implemented and followed 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).
- ✓ **Authorization for Certificate:** That, at the time of issuance, HARICA implemented and followed 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.
- ✓ **Accuracy of Information:** That, at the time of issuance, HARICA implemented and followed a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the `subject:organizationalUnitName` attribute).
- ✓ **No Misleading Information:** That, at the time of issuance, HARICA implemented and followed a procedure for reducing the likelihood that the information contained in the Certificate's `subject:organizationalUnitName` attribute would be misleading.
- ✓ **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, HARICA implemented and followed a procedure to verify the identity of the Applicant in accordance with section 3.2.
- ✓ **Subscriber Agreement:** That, if HARICA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies this CP/CPS, or, if HARICA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use.

9.6.3 Subscriber Representations and Warranties

HARICA SHALL require, as part of the Subscriber Agreement, that the Applicant make the commitments and warranties in this section for the benefit of HARICA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, HARICA SHALL obtain, for the express benefit of HARICA and the Certificate Beneficiaries, Applicant's agreement to the Subscriber Agreement or the Terms of Use.
The Subscriber Agreement or Terms of Use shall contain the following obligations and warranties:

- ✓ HARICA Subscribers are obliged to read, accept and comply with this Certificate Policy/Certification Practice Statement. Subscribers are obliged to use the certificates solely for the purposes described in this CP/CPS and the applicable law. HARICA Certificates cannot be used for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger of life.
- ✓ The Subscriber's request for certificate and issuance of the certificate itself is clear from any third-party intellectual property or proprietary rights, does not contain data which in any way interferes with or infringes upon the rights of any third party in any jurisdiction with respect to patents, trademarks, service marks, trade names, company names, "doing business as" (DBA) names and other trade rights, and does not present the data for any unlawful purpose whatsoever. Data covered by this representation and warranty includes but is not limited to any domain name, domain name space, Distinguished Name (DN), or Fully-Qualified Domain Name (FQDN), and/or any trade name or DBA name, contained in any part of the certificate request.
- ✓ With the exception of HARICA generating key pairs on behalf of Subscribers, Subscribers must create key pairs (private and public) using reliable and secure systems and must take all necessary precautions to protect their private keys from accidental destruction, loss or theft.
- ✓ After they receive their certificate, Subscribers agree and confirm that the information contained in the certificate, is accurate.
- ✓ Subscribers must request certificate revocation when it is not used anymore, when the data contained has changed or when it is suspected that the private key has been compromised or lost. Failure to request revocation of the Certificate, voids any liability claims if the private key or the Certificate is mis-used, when it should have been revoked.
- ✓ For TLS Certificates, when the Subscriber requests revocation, the most appropriate revocation reason should be selected, as described in section 4.9.1.1.
- ✓ **Accuracy of Information:** An obligation and warranty to always provide accurate and complete information to HARICA, both in the certificate request and as otherwise requested by HARICA in connection with the issuance of the Certificate(s) to be supplied by HARICA.
- ✓ **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.
- ✓ **Responsiveness:** An obligation to respond to HARICA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- ✓ **Acknowledgment and Acceptance:** An acknowledgment and acceptance that HARICA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if HARICA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

In the case of HARICA Code Signing Subscribers, in addition to the above obligations and warranties, the Subscriber Agreement or Terms of Use shall contain the following obligations and warranties:

- ✓ **Protection of Private Key:** Where the key is available outside a Signing Service, to maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 6.2.7.4, 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). HARICA SHALL provide the Subscriber with documentation on how to protect a Private Key. HARICA MAY provide this documentation as a set if instructions on the service web site or as a "white paper". The Subscriber SHALL represent that it will generate and operate any device storing private keys in a secure manner, as described in a document of code signing best practices, which HARICA SHALL provide to the Subscriber during the ordering process. HARICA SHALL obligate the Subscriber to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
- ✓ **Private Key Reuse:** Do not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.
- ✓ **Use:** To use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

- ✓ In the case of HARICA TSA Subscribers, they must verify that the requested TST has been signed by a TSU private key that corresponds to a valid HARICA TSU Certificate and check for possible revocations.

9.6.4 Relying Party Representations and Warranties

- ✓ HARICA Certificates cannot be used for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger of life.
- ✓ Entities that trust the issued certificates are obligated to read and accept this Certificate Policy/Certification Practice Statement and to use the certificates only in ways that conform to this CP/CPS and the current legislation.
- ✓ Entities that trust the certificates must check the validity of the digital certificate signature and trust the parent Certification Authorities. Finally, they should periodically check the validity of the certificate against the relevant Certificate Revocation List of use the Online Certificate Status Protocol (OCSP) service for possible revocations.
- ✓ Entities that trust the certificates must check the Extended Key Usage X.509 Extension in the End-Entity Certificate and Issuing CA Certificate for the appropriate use of the certificates.
- ✓ Collect enough information to determine the extent to which they can rely on a digital certificate
- ✓ Bear full and sole responsibility for any decision to rely on a digital certificate
- ✓ Bear the full consequences, including legal liability, for any failure to observe their obligations and responsibilities as detailed in this CP/CPS.

- ✓ Entities that trust the Time-Stamps must verify that the TST has been signed by a TSU private key that corresponds to a valid HARICA TSU Certificate and check for possible revocations and that the private key used to sign the time-stamp has not been compromised until the time of the verification. If this verification occurs after the expiration date of the TSU Certificates, the provisions of Annex D of ETSI EN 319 421 provide guidance.
- ✓ Entities that trust the Time-Stamps must consider any limitations of the usage of the time-stamp indicated by the time-stamp policy and consider any other precautions prescribed in agreements or elsewhere.
- ✓ Entities that trust the Time-Stamps as "Qualified", must use the designated EU "Trusted List" to establish whether the time-stamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of warranties

No stipulation

9.8 Limitations of liability

This clause applies to liability under contract (including under any indemnity or breach of warranty), in tort (including negligence), under statue or otherwise for non – compliant usage of the certificate(s) the associated private keys, the revocation status information or any other hardware or software provided, and any consequential, incidental, special, or exemplary damages arising out of or related to this CP/CPS, including but not limited to, loss of data, loss of business and loss of profit. Except as set out in the next paragraph, and to the extent permitted by applicable law, HARICA cannot and shall not be held liable for any problems or damages that may arise from its services in case of wrongful, negligent or improper use of the issued certificates. HARICA does not undertake any financial, civil or other responsibilities for such cases. Using HARICA and its certification services requires that users unconditionally accept the terms and services of this CP/CPS and that HARICA is not liable and does not undertake any financial, civil or other responsibilities, except for cases where there is evidence of fraudulent intent or serious negligence by HARICA or its operators. HARICA shall not be liable to the Subscriber for any loss suffered by the Subscriber due to use of a Certificate outside the normal and intended use. Subscribers are obliged to request Certificate revocation for reasons stated in section 9.6.3. Failure to request revocation of the Certificate, voids any liability claims if the private key or the Certificate is mis-used, when it should have been revoked with actions originating from the Subscriber.

If HARICA deviates significantly from the provisions set forth in this CP/CPS when issuing "**Certificates for Qualified electronic signatures**", "**Certificates for Qualified electronic seals**", "**Qualified Certificates for web site authentication**",

"**Extended Validation Certificates for SSL or Code Signing**", certain liability provisions apply:

- HARICA is only liable for the correct verification of the application and the resultant contents of the Certificate (except for the "OU" field as stated in section 9.6.2).
- HARICA shall not be liable if the Applicant/Subscriber supplied false or tampered validation evidence and information from this evidence was included in the Certificate. In this case, the Subscriber is liable for damage which HARICA and/or GUnet may suffer due to incorrect data being included in the Certificate or if the Subscriber uses such a Certificate in an incorrect way.

Except for the previous cases, HARICA's liability under this CP/CPS sustained by Subscribers or Relying Parties is limited to a maximum of **2.000€ per Certificate for Qualified Signatures/Seals, Qualified Certificates for website authentication, Extended Validation Certificates for SSL and Extended Validation Certificates for Code Signing** and a total maximum of claims of **1.000.000€**, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The Liability limitations provided in this paragraph shall be the same irrespective to the number of Certificates, transactions, or claims related to such Certificate. The limitations on Liability provided herein shall apply to the maximum extent allowed under the applicable Law of the applicable jurisdiction. This is covered via a Commercial General Liability combined with a Professional Liability/Errors and Omissions insurance, with policy limits of five million Euros (5.000.000€) in coverage, including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining Certificates for Qualified Signatures/Seals, Qualified Certificates for web site authentication, Extended Validation Certificates for SSL and Extended Validation Certificates for Code Signing, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

9.9 Indemnification

The Subscriber shall indemnify HARICA and its affiliates and their respective directors, officers, employees and agents (each an "Indemnified Person") against all liabilities, losses, expenses or costs (collectively "Losses") that, directly or indirectly are based on Subscriber's breach of this Agreement, any information, misrepresentation or breach of warranty or covenant provided by the Subscriber or Subscriber's or its customers' interference or infringement upon the rights of any third party and shall be responsible for defending all actions against an Indemnified.

The indemnification obligations of the Subscriber are not HARICA's sole remedy for Subscriber's breach and are in addition to any other remedies HARICA may have against the Subscriber under this Agreement. The Subscriber's indemnification obligations survive the termination of this Agreement.

HARICA 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 HARICA, 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 HARICA 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 HARICA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and termination

This CP/CPS is valid and effective for as long as HARICA is operational. When a Subordinate CA decides to terminate their services, and withdraw from HARICA, it must officially notify the Management Committee of HARICA. Similar correspondence is essential when an Organization wishes to participate and become a member of HARICA.

9.10.1 Term and termination for Subscriber Agreements

Term. Unless otherwise terminated as allowed in this CP/CPS, a Subscriber Agreement is effective upon Subscriber's acceptance and shall continue for as long as a Certificate issued under that Subscriber Agreement is valid.

Termination. Either Party may terminate the Subscriber Agreement for convenience by providing the other party twenty (20) business days' notice. HARICA may terminate a Subscriber Agreement immediately without notice if

(i) Subscriber materially breaches the Subscriber Agreement
(ii) HARICA revokes a Certificate as allowed in this CP/CPS
(iii) HARICA rejects Subscriber's Certificate application
(iv) HARICA cannot satisfactorily validate Subscriber in accordance with the provisions of this CP/CPS, or if
(v) industry standards or changes in applicable legislation affect the validity of the Certificates requested by the Subscriber.

9.11 Individual notices and communications with participants

Electronic mail, postal mail, fax, and web pages will all be valid means of providing any of the notices required by this CP/CPS, unless specifically provided otherwise. Notices by phone will be used as an additional method of communication whenever it is required (e.g. revocation procedure).

9.12 Amendments

All changes to this CP/CPS and other procedural documents, are supervised and must be approved by the HARICA PMC as described in section 1.5.1.

9.12.1 Procedure for amendment

Syntax changes can be made to the Certificate Policy and to the Certification Practice Statement without any prior notice to Subscribers and Application Software Suppliers.

9.12.2 Notification mechanism and period

In case of material changes to the CP/CPS, Subscribers will be notified in advance to the effective dates. HARICA is obligated to publish (at its web site), previous versions of its CP/CPS in case of material document changes. The most recent CP/CPS is always published at the following URL: https://repo.harica.gr/documents/CPS.

HARICA may

(i) revise the terms of the Subscriber Agreement; and/or
(ii) change part of the services provided herein at any time.

Any such change shall be notified to the Subscriber by any convenient way and in any case, shall be binding and effective fourteen (14) days after publication of the changes in the Subscriber Agreement and/or in the CP/CPS on HARICA'S web site https://repo.harica.gr, or upon notification to the Subscriber by email. If the Subscriber continuous to use its Certificate or Time-Stamping Services after the date on which the terms of the Subscriber Agreement have changed, HARICA will treat such use by the Subscriber as acceptance of the updated terms.

9.12.3 Circumstances under which OID must be changed

Any change of this CP/CPS shall produce a new identifier (OID) which is reported in section 1.2. Subscribers will be informed beforehand in case of important changes in the CP/CPS.

9.13 Dispute resolution provisions

If a dispute or difference arises in connection with, or out of the interpretation of the Certificate Policy/Certification Practice Statement and the operations of the Certification Authority then the Subscriber concerned may address this dispute to the HARICA Policy Management Committee and shall attempt to resolve or settle such dispute in an amicable way before commencement of any legal proceedings. HARICA Policy Management Committee is responsible to investigate all matters concerning complaints and disputes about the provisioning of the trust services. See also section 3.1.6.

Unless settled amicably, any disputes in connection with or arising out of this Certificate Policy and Certification Practice Statement of HARICA Public Key Infrastructure shall be referred and submitted to the Greek courts that are competent and the exclusive venue is Athens Greece.

9.14 Governing law

HARICA is mainly focused on serving the Hellenic Academic and Research Community. The operation of HARICA as well as the interpretation of the CP/CPS adheres to the Greek Legislation.

9.15 Compliance with applicable law

This Certificate Policy and Certification Practice Statement of HARICA Public Key Infrastructure shall be interpreted, construed and enforced in all respects in accordance with the applicable European and Greek legislation. All proceedings or legal action

arising from Certificate Policy and Certification Practice Statement of HARICA Public Key Infrastructure must be commenced in the exclusive jurisdiction of courts of Athens Greece.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation

9.16.2 Assignment

Relying Parties and Subscribers shall not assign any of their rights, interests or obligations hereunder (whether by operation of law or otherwise), without the prior written consent of HARICA. Any such attempted assignment shall be null and void. Subject to the foregoing, this CP/CPS shall be binding upon and inure to the benefit of the parties hereto, their successors and permitted assignees.

9.16.3 Severability

If any provision or provisions of this CP/CPS shall be held to be invalid, illegal or unenforceable for any reason whatsoever: (a) the validity, legality and enforceability of the remaining provisions of this CP/CPS (including, without limitation, each portion of any section, paragraph or sentence of this CP/CPS containing any such provision held to be invalid, illegal or unenforceable, that is not itself invalid, illegal or unenforceable) shall not in any way be affected or impaired thereby and shall remain enforceable to the fullest extent permitted by law; (b) such provision or provisions shall be deemed reformed to the extent necessary to conform to applicable law and to give the maximum effect of this CP/CPS; and (c) to the fullest extent possible.

For SSL/TLS Certificates, In the event of a conflict between this CP/CPS and a law, regulation or government order (hereinafter “Law”) of any jurisdiction in which HARICA operates or issues certificates, HARICA may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or SSL/TLS certificate issuances that are subject to that Law. In such event, prior to issuing a certificate under the modified requirement, HARICA shall update this CP/CPS and include a detailed reference to the Law requiring a modification of this CP/CPS, and the specific modification to this CP/CPS implemented by HARICA.

HARICA SHALL also (prior to issuing an SSL/TLS certificate under the modified requirement or, if a provision of the EV Guidelines is illegal under local government laws) notify the CA/Browser Forum of the relevant information newly added to this CP/CPS, so that the CA/Browser Forum may consider possible revisions to their requirements/guidelines accordingly. Any modification to HARICA’s practice enabled under this section SHALL be discontinued if and when the Law no longer applies, or the CA/Browser Forum Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to HARICA's CP/CPS and a notice to the CA/Browser Forum, as outlined above, SHALL be made within 90 days.

9.16.4 Enforcement

HARICA's failure to enforce or to require the performance at any time of any of the provisions of this CP/CPS shall not be construed to be a waiver of such provision and shall not affect either the validity of this CP/CPS or any part hereof or HARICA's right thereafter to enforce the same or each provision at any time of this CP/CPS.

9.16.5 Force Majeure

The occurrence of a Force Majeure event constituting a delay in the performance or fulfillment of any HARICA's obligation hereunder shall not be used as a right of the Relying parties or Subscriber or any third party to make a claim for compensation against HARICA neither HARICA shall be liable for any default or delay caused directly or indirectly due to Force Majeure. Force Majeure means the exceptional events or circumstances to the extent that they are beyond HARICA's reasonable control. Conditions beyond HARICA's reasonable control include but are not limited to natural disasters such as fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the Hellenic Republic, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of HARICA.

9.17 Other Provisions

No stipulation.

10 ANNEX A (HARICA Roots)

=== BEGIN HARICA ROOT CA 2015 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research
Institutions RootCA 2015
        Validity
            Not Before: Jul  7 10:11:21 2015 GMT
            Not After : Jun 30 10:11:21 2040 GMT
        Subject: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research
Institutions RootCA 2015
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:c2:f8:a9:3f:1b:89:fc:3c:3c:04:5d:3d:90:36:
                    b0:91:3a:79:3c:66:5a:ef:6d:39:01:49:1a:b4:b7:
                    cf:7f:4d:23:53:b7:90:00:e3:13:2a:28:a6:31:f1:
                    91:00:e3:28:ec:ae:21:41:ce:1f:da:fd:7d:12:5b:
                    01:83:0f:b9:b0:5f:99:e1:f2:12:83:80:4d:06:3e:
                    df:ac:af:e7:a1:88:6b:31:af:f0:8b:d0:18:33:b8:
                    db:45:6a:34:f4:02:80:24:28:0a:02:15:95:5e:76:
                    2a:0d:99:3a:14:5b:f6:cb:cb:53:bc:13:4d:01:88:
                    37:94:25:1b:42:bc:22:d8:8e:a3:96:5e:3a:d9:32:
                    db:3e:e8:f0:10:65:ed:74:e1:2f:a7:7c:af:27:34:
                    bb:29:7d:9b:b6:cf:09:c8:e5:d3:0a:fc:88:65:65:
                    74:0a:dc:73:1c:5c:cd:40:b1:1c:d4:b6:84:8c:4c:
                    50:cf:68:8e:a8:59:ae:c2:27:4e:82:a2:35:dd:14:
                    f4:1f:ff:b2:77:d5:87:2f:aa:6e:7d:24:27:e7:c6:
                    cb:26:e6:e5:fe:67:07:63:d8:45:0d:dd:3a:59:65:
                    39:58:7a:92:99:72:3d:9c:84:5e:88:21:b8:d5:f4:
                    2c:fc:d9:70:52:4f:78:b8:bd:3c:2b:8b:95:98:f5:
                    b3:d1:68:cf:20:14:7e:4c:5c:5f:e7:8b:e5:f5:35:
                    81:19:37:d7:11:08:b7:66:be:d3:4a:ce:83:57:00:
                    3a:c3:81:f8:17:cb:92:36:5d:d1:a3:d8:75:1b:e1:
                    8b:27:ea:7a:48:41:fd:45:19:06:ad:27:99:4e:c1:
                    70:47:dd:b5:9f:81:53:12:e5:b1:8c:48:5d:31:43:
                    17:e3:8c:c6:7a:63:96:4b:29:30:4e:84:4e:62:19:
```

```
                5e:3c:ce:97:90:a5:7f:01:eb:9d:e0:f8:8b:89:dd:
                25:98:3d:92:b6:7e:ef:d9:f1:51:51:7d:2d:26:c8:
                69:59:61:e0:ac:6a:b8:2a:36:11:04:7a:50:bd:32:
                84:be:2f:dc:72:d5:d7:1d:16:47:e4:47:66:20:3f:
                f4:96:c5:af:8e:01:7a:a5:0f:7a:64:f5:0d:18:87:
                d9:ae:88:d5:fa:84:c1:3a:c0:69:28:2d:f2:0d:68:
                51:aa:e3:a5:77:c6:a4:90:0e:a1:37:8b:31:23:47:
                c1:09:08:eb:6e:f7:78:9b:d7:82:fc:84:20:99:49:
                19:b6:12:46:b1:fb:45:55:16:a9:a3:65:ac:9c:07:
                0f:ea:6b:dc:1f:2e:06:72:ec:86:88:12:e4:2d:db:
                5f:05:2f:e4:f0:03:d3:26:33:e7:80:c2:cd:42:a1:
                17:34:0b
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            71:15:67:C8:C8:C9:BD:75:5D:72:D0:38:18:6A:9D:F3:71:24:54:0B
Signature Algorithm: sha256WithRSAEncryption
    75:bb:6d:54:4b:aa:10:58:46:34:f2:62:d7:16:36:5d:08:5e:
    d5:6c:c8:87:bd:b4:2e:46:f2:31:f8:7c:ea:42:b5:93:16:55:
    dc:a1:0c:12:a0:da:61:7e:0f:58:58:73:64:72:c7:e8:45:8e:
    dc:a9:f2:26:3f:c6:79:8c:b1:53:08:33:81:b0:56:13:be:e6:
    51:5c:d8:9b:0a:4f:4b:9c:56:53:02:e9:4f:f6:0d:60:ea:4d:
    42:55:e8:7c:1b:21:21:d3:1b:3a:cc:77:f2:b8:90:f1:68:c7:
    f9:5a:fe:fa:2d:f4:bf:c9:f5:45:1b:ce:38:10:2a:37:8a:79:
    a3:b4:e3:09:6c:85:86:93:ff:89:96:27:78:81:8f:67:e3:46:
    74:54:8e:d9:0d:69:e2:4a:f4:4d:74:03:ff:b2:77:ed:95:67:
    97:e4:b1:c5:ab:bf:6a:23:e8:d4:94:e2:44:28:62:c4:4b:e2:
    f0:d8:e2:29:6b:1a:70:7e:24:61:93:7b:4f:03:32:25:0d:45:
    24:2b:96:b4:46:6a:bf:4a:0b:f7:9a:8f:c1:ac:1a:c5:67:f3:
    6f:34:d2:fa:73:63:8c:ef:16:b0:a8:a4:46:2a:f8:eb:12:ec:
    72:b4:ef:f8:2b:7e:8c:52:c0:8b:84:54:f9:2f:3e:e3:55:a8:
    dc:66:b1:d9:e1:5f:d8:b3:8c:59:34:59:a4:ab:4f:6c:bb:1f:
    18:db:75:ab:d8:cb:92:cd:94:38:61:0e:07:06:1f:4b:46:10:
    f1:15:be:8d:85:5c:3b:4a:2b:81:79:0f:b4:69:9f:49:50:97:
    4d:f7:0e:56:5d:c0:95:6a:c2:36:c3:1b:68:c9:f5:2a:dc:47:
    9a:be:b2:ce:c5:25:e8:fa:03:b9:da:f9:16:6e:91:84:f5:1c:
    28:c8:fc:26:cc:d7:1c:90:56:a7:5f:6f:3a:04:bc:cd:78:89:
    0b:8e:0f:2f:a3:aa:4f:a2:1b:12:3d:16:08:40:0f:f1:46:4c:
    d7:aa:7b:08:c1:0a:f5:6d:27:de:02:8f:ca:c3:b5:2b:ca:e9:
    eb:c8:21:53:38:a5:cc:3b:d8:77:37:30:a2:4f:d9:6f:d1:f2:
    40:ad:41:7a:17:c5:d6:4a:35:89:b7:41:d5:7c:86:7f:55:4d:
    83:4a:a5:73:20:c0:3a:af:90:f1:9a:24:8e:d9:8e:71:ca:7b:
    b8:86:da:b2:8f:99:3e:1d:13:0d:12:11:ee:d4:ab:f0:e9:15:
```

```
        76:02:e4:e0:df:aa:20:1e:5b:61:85:64:40:a9:90:97:0d:ad:
        53:d2:5a:1d:87:6a:00:97:65:62:b4:be:6f:6a:a7:f5:2c:42:
        ed:32:ad:b6:21:9e:be:bc
```

=== END HARICA ROOT CA 2015 ===

=== BEGIN HARICA ECC ROOT CA 2015 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research
Institutions ECC RootCA 2015
        Validity
            Not Before: Jul  7 10:37:12 2015 GMT
            Not After : Jun 30 10:37:12 2040 GMT
        Subject: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research
Institutions ECC RootCA 2015
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:92:a0:41:e8:4b:82:84:5c:e2:f8:31:11:99:86:
                    64:4e:09:25:2f:9d:41:2f:0a:ae:35:4f:74:95:b2:
                    51:64:6b:8d:6b:e6:3f:70:95:f0:05:44:47:a6:72:
                    38:50:76:95:02:5a:8e:ae:28:9e:f9:2d:4e:99:ef:
                    2c:48:6f:4c:25:29:e8:d1:71:5b:df:1d:c1:75:37:
                    b4:d7:fa:7b:7a:42:9c:6a:0a:56:5a:7c:69:0b:aa:
                    80:09:24:6c:7e:c1:46
                ASN1 OID: secp384r1
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                B4:22:0B:82:99:24:01:0E:9C:BB:E4:0E:FD:BF:FB:97:20:93:99:2A
    Signature Algorithm: ecdsa-with-SHA256
         30:64:02:30:67:ce:16:62:38:a2:ac:62:45:a7:a9:95:24:c0:
         1a:27:9c:32:3b:c0:c0:d5:ba:a9:e7:f8:04:43:53:85:ee:52:
         21:de:9d:f5:25:83:3e:9e:58:4b:2f:d7:67:13:0e:21:02:30:
         05:e1:75:01:de:68:ed:2a:1f:4d:4c:09:08:0d:ec:4b:ad:64:
         17:28:e7:75:ce:45:65:72:21:17:cb:22:41:0e:8c:13:98:38:
         9a:54:6d:9b:ca:e2:7c:ea:02:58:22:91
```

=== END HARICA ECC ROOT CA 2015 ===

=== BEGIN HARICA Client ECC Root CA 2021 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            31:68:d9:d8:e1:62:57:1e:d2:19:44:88:e6:10:7d:f0
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Client ECC Root CA 2021
        Validity
            Not Before: Feb 19 11:03:34 2021 GMT
            Not After : Feb 13 11:03:33 2045 GMT
        Subject: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Client ECC Root CA 2021
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:07:18:ad:95:96:94:d0:5c:0f:82:f7:2a:40:fa:
                    02:c9:c9:3d:36:a6:a3:04:6a:c1:6d:95:01:88:60:
                    12:54:6c:5c:a2:2b:6e:13:3a:88:95:0c:1c:26:86:
                    36:4a:89:19:b7:18:de:3b:e8:a8:50:1f:ca:df:5b:
                    bf:49:80:15:db:e3:30:e1:1d:5a:c7:2a:8a:01:07:
                    fe:6d:2c:34:ef:28:28:97:bc:c1:f9:57:86:95:8b:
                    35:cf:9e:5a:d1:68:95
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                52:08:D2:BE:32:81:25:FD:F5:1A:97:EC:4E:5F:1A:BB:53:CD:90:AD
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA384
         30:64:02:30:4c:31:45:46:4f:a8:e6:be:c3:77:b2:1a:18:4b:
         2d:88:7b:58:e6:ab:94:6b:44:03:b0:17:ff:df:82:73:44:51:
         2c:fd:93:1d:06:7b:14:d2:89:ec:40:0c:ef:21:01:2e:02:30:
         2f:c9:2e:5a:6c:2c:1d:d9:95:e0:9e:b0:b9:5c:52:7c:f6:f8:
         38:ca:2e:f1:d4:1d:f2:a2:49:a2:95:f8:c1:58:5e:4f:fe:73:
         0a:ef:31:b0:ab:23:58:13:8c:8b:de:3b
```

=== END HARICA Client ECC Root CA 2021 ===

=== BEGIN HARICA Client RSA Root CA 2021 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            55:52:f8:1e:db:1b:24:2c:9e:bb:96:18:cd:02:28:3e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Client RSA Root CA 2021
        Validity
            Not Before: Feb 19 10:58:46 2021 GMT
            Not After : Feb 13 10:58:45 2045 GMT
        Subject: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Client RSA Root CA 2021
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:81:db:57:42:90:2c:74:35:f4:f8:b8:74:19:4d:
                    ab:09:5a:77:45:81:73:62:b0:35:9f:f8:d0:b7:33:
                    00:87:13:b6:96:ab:0e:54:12:30:07:bc:9b:b7:48:
                    d7:d1:19:83:ae:8e:d8:a9:f1:a9:00:84:b0:8c:5e:
                    9e:e8:0c:8f:54:69:bf:f6:d4:08:4f:26:70:fe:18:
                    41:63:1a:b3:32:8b:40:f8:07:ab:57:31:f0:c6:16:
                    76:67:9a:b4:dd:2f:f2:d1:6b:c5:d0:92:84:91:71:
                    6e:0f:2e:63:e9:1f:53:a4:dd:52:13:cc:09:83:29:
                    81:0c:c5:53:75:44:b1:0e:67:53:18:d0:c3:1f:88:
                    4b:9f:94:24:b4:29:bc:bb:e8:4e:fd:6f:d2:15:1d:
                    49:dc:8d:70:f2:11:1a:20:51:55:11:ba:88:6f:c4:
                    f7:50:79:d6:aa:31:e2:84:3d:5e:32:c8:77:2a:50:
                    71:e5:0b:2f:e9:b6:ea:ef:ab:0a:33:39:0e:fd:8f:
                    a5:67:43:82:8e:98:69:09:09:1b:40:cd:38:67:47:
                    ea:c9:ec:97:71:12:de:24:f5:72:3c:d1:f7:43:4c:
                    26:f7:90:b2:89:e9:45:4b:55:3d:31:05:7a:41:e2:
                    95:ba:43:c0:17:c5:b6:85:3d:19:8d:64:70:f3:5b:
                    ac:cd:9f:d3:29:75:87:4b:95:67:6a:a6:f8:d1:dd:
                    bc:90:86:89:43:29:a9:37:5b:f5:5d:b0:26:5a:53:
                    42:76:90:2b:cf:9e:56:6c:2b:54:cf:5c:9a:65:df:
                    5b:8b:48:60:38:7c:fb:c5:0b:cf:76:04:63:02:33:
                    2a:7d:f5:83:67:e7:fa:c6:43:fd:2b:0f:d4:26:2f:
                    77:a4:32:c1:24:ea:64:9d:bf:b3:38:71:31:44:f2:
                    47:b8:a2:66:41:a1:fb:9b:7b:bc:c7:46:6a:75:bf:
                    5a:a2:8c:e8:6a:44:c1:b8:96:b5:c0:32:08:2d:7b:
                    74:35:73:b2:ca:c6:fe:af:11:72:18:f6:e7:c8:c2:
                    cf:a5:2a:ea:7b:d6:59:e8:7c:a0:b2:6a:40:09:69:
                    0e:a5:96:db:d1:00:b9:f1:88:6e:36:f0:88:b2:9d:
                    f1:52:f2:c3:7c:bf:30:89:3c:0a:69:f9:22:a4:65:
                    e1:9b:e0:74:c6:b1:85:97:96:2c:ae:94:8f:50:a6:
                    39:12:1f:be:47:f2:81:78:d3:75:36:9e:7d:5a:20:
                    97:e2:52:ae:99:9f:c6:7c:9b:66:f3:fe:d8:cf:ee:
```

```
                    bd:97:06:1d:2d:85:dc:3e:36:53:96:7b:20:ba:e8:
                    c8:e1:ad:96:62:3e:11:7c:b3:00:84:9e:a7:4c:71:
                    ab:4a:37
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Basic Constraints: critical
                    CA:TRUE
                X509v3 Subject Key Identifier:
                    A0:D6:07:3D:5E:24:F7:7B:A0:44:2E:24:52:0D:19:AA:2B:04:91:A7
                X509v3 Key Usage: critical
                    Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
         0d:47:f9:09:66:31:52:ec:79:ee:c2:a8:f2:68:3e:ed:96:45:
         cb:3a:a6:98:63:3f:ea:2b:4d:4e:03:d0:1c:82:e1:cb:d3:e5:
         d6:ab:5b:67:28:bc:9d:fe:0c:99:0a:80:55:a7:ce:1b:23:61:
         0d:b0:57:f0:fe:e0:ca:be:e6:90:db:83:2c:be:83:8e:f4:79:
         b6:fe:d0:0d:42:a7:58:1f:69:ea:81:f5:05:a5:fe:46:68:eb:
         6c:78:c9:e0:ea:e7:e6:de:31:c5:d2:d5:2c:82:63:28:9d:5d:
         a8:1a:7e:88:e6:e7:2b:f1:2c:d5:d0:05:9e:dc:2d:bd:37:66:
         d4:04:a2:a7:ad:bf:3a:c2:a8:3b:ad:ff:8d:9d:33:e0:b9:9a:
         84:a1:87:1f:76:f4:82:74:d7:0e:f9:30:48:3e:5b:88:3e:aa:
         5c:6b:d6:2f:0c:e8:8e:73:c2:18:91:83:39:b6:66:5a:d0:1f:
         60:27:5d:4d:e3:f6:3a:0d:66:50:9c:78:7b:ab:f3:13:10:ae:
         0f:2f:ab:e8:64:b3:18:20:9d:46:35:64:25:73:ea:9b:10:5c:
         58:35:89:b1:46:48:a7:f4:ac:d4:1d:9e:5b:cc:a9:a5:1a:13:
         4f:24:50:aa:d9:1b:6d:b1:40:fb:9d:dd:58:74:c4:c2:6f:14:
         72:ec:db:35:9f:b8:54:75:45:c3:a6:c8:1a:28:35:3a:ae:65:
         f2:a9:98:ce:af:5b:c9:38:8c:31:3b:7f:cc:dc:96:fd:e2:5b:
         d6:d0:59:f4:76:ba:0b:cb:4f:83:10:c7:40:d0:1d:60:e9:2a:
         e5:48:58:77:0c:45:69:be:19:71:04:24:e2:e3:24:1f:4a:c8:
         c1:3e:99:f5:96:98:38:48:25:a1:15:b0:1b:d7:e2:84:18:5b:
         f6:71:35:9a:68:7b:40:cc:18:5c:0c:24:9d:d4:95:f5:99:aa:
         46:ea:ae:ac:bf:f4:14:19:24:e8:8c:ec:e3:f5:bc:06:68:8a:
         2a:0c:05:5f:0a:97:75:a7:dc:7e:c0:fd:d7:7a:18:df:30:d1:
         38:4b:1f:b0:98:70:bf:cc:7c:73:f0:6e:c4:31:a5:a4:97:1d:
         ac:bf:ce:6c:21:4a:be:27:23:67:f3:06:56:81:0a:91:8e:b6:
         e1:03:05:33:2c:da:34:08:4d:4e:50:23:ad:1f:a5:c5:d4:7a:
         fe:ea:09:ec:a7:28:60:8b:46:7c:b5:ea:9b:dd:4f:f9:e7:6b:
         15:c6:88:cf:43:db:e5:27:dc:04:56:6e:6f:46:15:f1:56:2d:
         e8:5c:0c:73:c3:23:81:38:20:cb:c9:0c:69:cf:2c:ab:3b:84:
         60:33:19:52:fd:69:14:33
```

=== END HARICA Client RSA Root CA 2021 ===

=== BEGIN HARICA Code Signing ECC Root CA 2021 ===

```
Certificate:
    Data:
```

```
        Version: 3 (0x2)
        Serial Number:
            4c:8a:63:1d:a9:63:8f:05:a2:fb:76:14:ff:5b:a2:cd
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Code Signing ECC Root CA 2021
        Validity
            Not Before: Feb 19 11:04:36 2021 GMT
            Not After : Feb 13 11:04:35 2045 GMT
        Subject: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Code Signing ECC Root CA 2021
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:43:9f:bc:5c:42:6a:43:e1:ac:4b:b8:0e:5f:80:
                    06:e3:05:77:8b:7f:0b:79:d7:61:a0:90:bf:f2:53:
                    28:a3:58:ba:94:c0:66:6a:1c:59:da:80:58:81:00:
                    4c:bc:c9:79:98:10:0c:c7:1d:0b:e3:93:dc:85:39:
                    68:d9:bf:a7:43:d2:31:cc:82:82:27:ba:88:d1:d2:
                    2d:56:37:f7:3a:da:6e:39:dc:71:10:65:ee:38:0b:
                    87:7a:03:ba:30:5f:64
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                6A:71:C1:73:6A:93:42:A6:97:72:5E:BB:90:5F:82:92:0F:2B:D6:EB
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA384
         30:64:02:30:1e:a5:d5:0b:44:95:10:e4:67:7c:4e:85:5e:b9:
         45:49:02:73:b0:b2:1c:b3:a7:22:d1:00:61:40:0f:b3:87:37:
         16:8d:00:ed:b6:8b:55:25:06:94:90:dc:d7:e7:75:9f:02:30:
         7f:74:6b:f1:4a:df:f0:f7:84:7b:f2:c5:79:30:03:48:f2:1e:
         20:22:57:64:54:57:34:80:77:b7:3f:23:4f:b4:f5:80:98:c2:
         c1:56:5b:a0:e7:d6:a1:8f:f5:0c:6f:1d
```

=== END HARICA Code Signing ECC Root CA 2021 ===

=== BEGIN HARICA Code Signing RSA Root CA 2021 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            15:c2:ae:2a:4d:99:9a:63:8c:d3:ba:13:19:76:08:f5
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Code Signing RSA Root CA 2021
```

```
Validity
    Not Before: Feb 19 10:59:54 2021 GMT
    Not After : Feb 13 10:59:53 2045 GMT
Subject: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA Code Signing RSA Root CA 2021
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (4096 bit)
        Modulus:
            00:8a:6a:ee:aa:0a:23:55:0c:8b:06:42:e3:95:5b:
            54:78:5f:c5:8e:06:2c:7c:3c:31:be:af:0d:a9:a1:
            ec:4a:20:58:05:9d:e2:68:b2:bb:eb:5f:7f:2a:33:
            b9:f2:55:9c:6f:aa:a4:1e:ed:10:be:83:29:11:36:
            e6:9e:3f:fa:6d:7b:51:e1:d5:77:a5:bd:cb:69:0e:
            3b:22:20:94:0c:31:65:40:0d:09:af:10:35:7a:9b:
            ea:79:08:44:a4:8b:67:a9:2b:4d:c1:e7:d0:d7:a7:
            f6:b5:3a:8d:d9:a3:a9:79:b8:a4:65:5c:bc:f3:3e:
            f7:9f:99:f6:b8:c3:65:68:2d:ab:83:2e:dd:85:99:
            04:a9:f5:d1:5c:d5:51:42:01:b9:9f:41:b5:4b:22:
            b2:00:f4:cb:67:10:ef:69:c4:10:ad:fa:94:06:76:
            50:12:57:82:ae:c5:14:ad:3c:7d:bb:9d:f1:73:e1:
            7c:f0:ae:71:de:5b:f7:12:dd:f7:80:f1:dc:3e:f1:
            60:ba:c9:19:97:6f:75:74:85:4c:fd:39:43:c3:64:
            6e:34:ac:13:c1:1c:65:b6:52:42:f1:46:eb:2f:fa:
            5d:a6:cf:0e:49:9d:f7:74:7c:78:0d:06:3a:2c:12:
            fb:e2:4b:26:e4:6f:8b:21:81:33:42:39:13:e8:42:
            ab:5b:55:d4:1b:bb:37:b6:12:91:f7:f3:7d:bc:d2:
            ff:ec:b1:c3:d5:a0:cc:b2:2b:c7:8f:5d:7e:4c:52:
            42:48:fb:8f:fd:5a:90:73:10:d5:a9:72:54:8d:49:
            db:38:52:aa:46:48:0e:2f:fa:00:2c:cc:73:0c:36:
            4b:24:ce:13:6c:a6:a4:a4:a3:d6:7c:9b:e9:38:0b:
            c6:24:db:4d:ac:67:21:49:5b:41:37:64:e6:60:6b:
            1f:ed:2a:2f:60:19:30:1e:d8:3c:9c:19:43:87:df:
            c0:0a:f4:e4:ca:60:88:7a:d6:a3:b9:e4:25:2e:79:
            e2:fe:c1:cb:3c:b7:f7:cf:4e:58:4c:fb:c3:ad:ab:
            7d:aa:ca:88:fb:0e:38:0d:1f:9e:5c:39:eb:b8:07:
            c4:50:22:4d:f8:85:7f:6e:ec:8c:fa:b6:71:4d:de:
            7d:96:69:c4:dd:3e:1e:de:26:90:0a:2c:4d:15:95:
            a9:a2:3e:dc:3d:0e:77:7c:8d:41:28:4f:b8:83:51:
            be:3e:b7:8f:90:3a:70:31:89:5a:fa:93:53:fc:60:
            c9:8d:75:90:ee:5a:2f:1d:84:9f:00:a9:e6:c3:86:
            23:a2:1e:dd:12:e3:a1:46:60:1b:67:bf:50:15:22:
            92:7c:4a:b4:8c:8f:6e:9c:95:c2:2c:dc:3b:3a:20:
            b6:bc:8b
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:TRUE
```

```
            X509v3 Subject Key Identifier:
                B4:64:16:48:E8:FC:5A:4B:33:29:89:EB:99:40:B9:20:B4:F6:61:1A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
         2b:ac:59:8b:e6:39:44:dc:fb:ad:4a:88:e0:64:ff:ab:c3:f2:
         d2:ce:70:2f:03:e5:6f:b2:c4:f5:36:d6:53:6b:87:ab:1d:8b:
         99:07:c8:30:8e:47:72:fd:a1:b8:75:d6:17:a1:16:bd:64:73:
         91:30:57:ad:7d:fd:05:40:86:93:d1:49:96:b2:0b:d4:7c:64:
         13:8b:d3:21:49:38:bb:fb:e8:cc:3e:31:f1:ae:7b:4c:2a:df:
         82:06:a3:8e:05:84:9c:7f:70:ce:c0:bb:45:17:df:5d:65:0c:
         e4:50:48:07:44:8b:a4:2f:56:da:c6:7a:f6:60:8d:a4:38:f1:
         9d:87:16:30:b2:f0:5f:7a:42:55:20:71:cf:cc:ee:00:b1:12:
         47:bf:42:b9:e4:b3:b5:1d:19:84:b9:98:6d:e0:69:b4:15:41:
         b5:e2:50:48:c7:1f:ea:9a:b7:79:91:dd:d5:d5:53:19:fc:ae:
         18:6c:69:db:ad:59:28:9b:64:98:a7:3c:c7:55:8e:d1:30:00:
         cf:d4:32:9e:62:b1:c3:2a:ee:35:22:c6:bb:f0:7c:bb:83:b8:
         00:89:f5:dc:1a:97:d9:38:9a:29:53:61:19:a6:a7:f4:3b:47:
         fd:dd:67:95:0f:8e:a4:66:2c:82:9a:b7:2d:71:e6:df:ae:f8:
         f8:68:c1:bb:0f:ea:50:a0:45:97:b7:1a:95:12:6f:c8:b3:b6:
         05:68:da:6a:1e:0e:35:85:84:ac:74:0c:8a:b4:f4:75:9f:22:
         af:b0:54:bb:b6:9e:22:f9:d9:eb:d5:8a:0d:c7:dc:f8:98:31:
         5f:9e:fa:c6:97:f4:41:10:75:d3:81:b6:31:5f:7a:dd:88:85:
         08:af:70:47:02:37:7b:e2:4a:ec:5d:f2:dd:29:12:44:c8:8a:
         aa:dd:d2:55:78:17:75:af:71:69:0d:77:70:4a:b0:1f:7f:42:
         db:c7:71:dc:58:d6:18:bd:50:c5:b9:72:04:c7:67:7b:7c:53:
         60:ca:49:18:15:bc:40:73:ae:2b:a8:2b:ac:6f:11:44:39:ec:
         82:48:7e:11:ca:fb:d6:3f:b6:c0:b9:b8:06:93:75:bd:93:27:
         77:17:0d:5c:a5:9e:ea:c1:5b:00:2d:0c:a8:35:60:c7:e2:6f:
         35:1b:3d:76:b5:e7:ad:dd:74:23:4f:86:b2:47:ef:c8:2f:d0:
         85:7c:39:96:37:a1:2b:29:02:bd:3e:87:cf:a8:f6:1d:75:32:
         cf:38:e3:73:b1:ee:10:81:b5:2a:b1:88:06:51:1e:5a:3a:48:
         51:f3:36:59:62:df:42:66:59:50:b7:58:be:f5:76:40:9a:12:
         16:e6:0e:aa:d7:6c:a0:d5
```

=== END HARICA Code Signing RSA Root CA 2021 ===

=== BEGIN HARICA Qualified ECC Root CA 2021 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            11:2c:97:28:ef:e7:89:f2:ff:7e:17:6d:c9:62:21:6e
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = GR, O = Greek Universities Network (GUnet), organizationIdentifier = VATGR-099028220, OU = Hellenic Academic and
Research Institutions CA, CN = HARICA Qualified ECC Root CA 2021
        Validity
```

```
            Not Before: Feb 19 11:02:27 2021 GMT
            Not After : Feb 13 11:02:26 2045 GMT
        Subject: C = GR, O = Greek Universities Network (GUnet), organizationIdentifier = VATGR-099028220, OU = Hellenic Academic and
Research Institutions CA, CN = HARICA Qualified ECC Root CA 2021
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:d1:f2:a6:d5:01:15:a0:9b:3f:16:a5:57:49:28:
                    d5:b5:fe:c7:07:49:5a:d8:d2:f4:d3:f1:01:89:6c:
                    7f:9d:ee:bc:63:6c:f0:5f:3d:8a:49:a5:b1:98:51:
                    38:24:56:ec:37:5b:f2:d5:87:96:47:46:c6:7a:fb:
                    dd:95:7b:5d:0d:a7:fd:a1:28:48:d9:01:bf:1e:4a:
                    91:29:2c:a0:b7:f8:09:42:c5:13:96:80:fd:28:36:
                    4c:11:09:c3:26:cb:f8
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                1F:35:FA:66:C3:B4:D0:9A:4A:24:82:7F:9B:28:8D:DA:9B:EE:E1:A6
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA384
         30:64:02:30:1d:49:12:7f:25:7c:6b:15:27:bb:b3:0a:f3:43:
         61:2d:65:b7:cf:24:d1:14:e5:1c:f6:aa:16:f7:20:91:ab:be:
         81:62:77:6e:5a:e5:be:31:43:8b:5d:65:13:bb:36:9b:02:30:
         0c:9e:b2:39:7d:30:c1:a7:31:6c:13:df:38:6a:51:85:c8:3f:
         d1:3a:30:c0:15:a4:02:3a:21:58:13:2d:db:67:a1:0f:7a:dd:
         32:86:53:43:0a:93:e7:c1:6f:95:2e:05
```

=== END HARICA Qualified ECC Root CA 2021 ===

=== BEGIN HARICA Qualified RSA Root CA 2021 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            32:be:30:39:72:57:46:d9:23:89:91:c2:36:7a:80:47
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GR, O = Greek Universities Network (GUnet), organizationIdentifier = VATGR-099028220, OU = Hellenic Academic and
Research Institutions CA, CN = HARICA Qualified RSA Root CA 2021
        Validity
            Not Before: Feb 19 10:57:38 2021 GMT
            Not After : Feb 13 10:57:37 2045 GMT
```

```
        Subject: C = GR, O = Greek Universities Network (GUnet), organizationIdentifier = VATGR-099028220, OU = Hellenic Academic and
Research Institutions CA, CN = HARICA Qualified RSA Root CA 2021
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:8f:44:67:d7:b6:ff:51:35:d2:18:32:6b:3b:ae:
                    d4:0a:4c:3e:a3:d0:60:71:ab:53:b6:dd:b5:91:2d:
                    18:e9:65:6d:82:6e:1f:9b:ff:d5:58:2f:e7:0c:50:
                    b2:b4:dc:56:10:44:a9:6f:d1:45:28:75:13:6d:99:
                    94:77:e4:45:61:54:b1:f3:bb:c4:e6:7f:fb:fb:ee:
                    7c:c5:a8:f9:f8:25:1b:02:7d:2a:55:91:39:a6:18:
                    b2:ea:fe:53:a4:70:ea:1d:f4:8b:08:73:a6:b9:a6:
                    7c:6b:42:50:18:95:45:ee:d5:94:06:3e:81:2b:df:
                    6f:ed:ee:8a:5c:74:59:cc:a0:b3:67:1e:56:7e:7b:
                    09:3e:ee:5b:d2:d3:89:57:52:40:5a:18:99:22:8b:
                    68:c3:c5:34:74:b8:2c:ac:69:7e:7e:3b:85:a9:29:
                    3e:dd:b9:0b:1c:7c:b8:88:f6:85:03:8f:64:80:ef:
                    50:ac:af:5a:90:06:18:54:cf:61:0b:5a:ea:0e:40:
                    78:75:68:48:0a:1d:35:2e:78:f0:32:f6:26:cf:1b:
                    5b:aa:49:2d:c0:39:ac:e6:5f:79:46:bd:36:94:9f:
                    18:52:74:f4:4c:9a:a6:ab:6a:4f:47:bb:a3:06:3d:
                    48:5d:95:e9:60:4e:2a:88:ac:9d:c0:75:9e:86:b9:
                    1f:e6:b0:3e:cf:cd:02:65:a5:b3:bf:a8:73:24:b2:
                    24:be:67:4e:04:6e:28:e5:df:f1:d4:bb:19:83:ed:
                    8f:ee:ba:b2:57:d2:0c:f6:04:e5:90:7f:09:5c:1d:
                    09:4d:31:a0:f9:e1:45:c2:08:77:ab:94:56:3f:90:
                    ae:79:91:1f:c8:b6:75:57:60:0b:f3:05:36:9c:2d:
                    52:52:b1:f3:e6:f6:d0:10:4e:2d:89:d1:e0:a8:41:
                    6f:c9:48:a2:0f:c7:c0:36:13:1f:6a:0d:51:cf:d9:
                    3c:08:eb:dd:0a:08:4e:cb:37:11:5d:38:84:ce:6e:
                    db:3e:a3:86:48:96:de:a5:04:ad:37:58:e0:68:48:
                    12:d4:7a:bc:26:6d:0c:5c:be:a9:6d:7a:0c:2b:31:
                    2b:09:ec:48:ed:4f:b0:a9:be:e3:54:ef:a0:8e:61:
                    09:4a:0a:c1:d7:6c:de:bd:70:ff:07:ed:c1:cb:08:
                    e0:ff:e0:02:bc:97:87:e7:cd:34:2b:02:5a:ac:f2:
                    b7:b1:0b:cf:1b:e7:15:ee:2e:be:6b:9e:c4:b0:c3:
                    c0:89:d6:81:a8:ae:89:a8:00:30:c7:33:6e:65:2d:
                    02:4e:18:0d:41:c4:ac:9f:7a:d1:45:bb:bc:c1:0b:
                    e3:a3:af:e5:d3:62:5c:f0:75:95:c0:66:b3:70:22:
                    81:2f:13
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                FC:24:46:39:57:2F:29:BE:48:EB:15:0D:76:FF:17:BF:DB:1C:9E:D7
```

```
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
         6e:e1:65:b3:6c:1e:c3:9c:50:1a:ff:0d:1c:b7:92:06:7c:58:
         0e:7b:0f:bc:53:56:6d:0e:84:01:cf:4f:03:61:c6:5b:b3:9b:
         d1:ee:06:e7:49:5c:d8:ad:f5:ec:38:40:e1:ef:b9:da:40:8c:
         fd:d6:db:70:54:c5:55:dd:1d:9e:2e:17:6e:1e:b0:09:ab:26:
         29:21:34:30:a4:3b:99:87:26:92:7e:18:f8:44:45:02:6f:96:
         a4:09:60:2d:69:df:6e:bc:46:45:a4:29:00:73:83:13:bd:45:
         c6:62:e0:a7:be:d0:1a:8f:0f:56:0f:da:35:fb:f9:f5:ef:6e:
         41:d5:a3:b4:10:e1:0c:2d:cb:03:3a:e7:75:1e:a5:e0:2b:dc:
         6a:84:a7:cd:33:65:70:89:6f:b3:93:b8:98:40:0c:35:fd:e0:
         97:3a:6a:7f:90:a4:47:f5:7a:c6:45:22:2f:f9:48:63:61:06:
         fe:7e:cf:7f:de:5b:a5:e7:a1:5b:19:40:3b:cd:cf:b2:e6:b8:
         ef:52:be:6e:16:3f:7a:e8:75:a1:3b:e0:01:be:d0:10:0a:62:
         c1:db:80:af:7f:f6:13:09:7d:2c:3d:45:53:71:94:f4:dc:99:
         34:8f:75:79:9b:72:d9:c0:91:5a:70:4b:21:55:01:d1:26:82:
         86:ff:c1:90:cb:7f:48:9a:b7:78:da:7d:93:e4:d1:72:b8:62:
         6b:25:09:d0:dc:61:60:85:98:85:14:0b:e7:18:e4:70:29:b8:
         7b:36:6c:8f:73:ed:20:79:fc:bb:9d:12:b6:a2:e6:17:01:9e:
         77:6a:0e:2a:ad:a4:04:d7:d5:19:9c:68:92:06:80:6d:b1:6c:
         e5:03:e0:73:f4:64:b6:4a:b2:80:ad:0f:21:00:44:0c:8b:b2:
         80:25:36:11:bf:e2:d0:1d:13:af:ac:b4:6b:79:d6:41:42:09:
         db:39:8c:1f:ab:21:f7:9a:90:7a:ba:49:cd:0c:e0:42:2d:c4:
         c2:ae:db:20:9b:8d:94:2b:ed:c8:0b:e6:f6:9a:14:1f:ea:0a:
         8d:55:65:74:58:0b:02:d2:cc:7e:60:1c:49:bd:25:58:9e:ec:
         4b:b2:ac:92:12:25:2c:91:78:1a:50:70:ff:0b:ec:10:76:6d:
         76:2f:73:aa:19:32:49:5b:9d:2b:ba:a6:50:62:2f:a7:0e:19:
         73:39:74:5e:b1:45:7d:14:2d:ee:cf:bd:b8:4b:22:6f:6a:81:
         fb:ac:64:0a:15:a4:d4:c2:03:2e:b0:ac:fc:bf:3e:a4:63:2f:
         2e:f4:c6:f6:e6:36:ad:e7:7b:fb:ef:2c:1f:f0:10:c5:8d:c5:
         c4:41:ce:e0:92:2a:2d:9e
```

=== END HARICA Qualified RSA Root CA 2021 ===

=== BEGIN HARICA TLS ECC Root CA 2021 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            67:74:9d:8d:77:d8:3b:6a:db:22:f4:ff:59:e2:bf:ce
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA TLS ECC Root CA 2021
        Validity
            Not Before: Feb 19 11:01:10 2021 GMT
            Not After : Feb 13 11:01:09 2045 GMT
        Subject: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA TLS ECC Root CA 2021
```

```
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:38:08:fe:b1:a0:96:d2:7a:ac:af:49:3a:d0:c0:
                    e0:c3:3b:28:aa:f1:72:6d:65:00:47:88:84:fc:9a:
                    26:6b:aa:4b:ba:6c:04:0a:88:5e:17:f2:55:87:fc:
                    30:b0:34:e2:34:58:57:1a:84:53:e9:30:d9:a9:f2:
                    96:74:c3:51:1f:58:49:31:cc:98:4e:60:11:87:75:
                    d3:72:94:90:4f:9b:10:25:2a:a8:78:2d:be:90:41:
                    58:90:15:72:a7:a1:b7
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                C9:1B:53:81:12:FE:04:D5:16:D1:AA:BC:9A:6F:B7:A0:95:19:6E:CA
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA384
         30:64:02:30:11:de:ae:f8:dc:4e:88:b0:a9:f0:22:ad:c2:51:
         40:ef:60:71:2d:ee:8f:02:c4:5d:03:70:49:a4:92:ea:c5:14:
         88:70:a6:d3:0d:b0:aa:ca:2c:40:9c:fb:e9:82:6e:9a:02:30:
         2b:47:9a:07:c6:d1:c2:81:7c:ca:0b:96:18:41:1b:a3:f4:30:
         09:9e:b5:23:28:0d:9f:14:b6:3c:53:a2:4c:06:69:7d:fa:6c:
         91:c6:2a:49:45:e6:ec:b7:13:e1:3a:6c
```

=== END HARICA TLS ECC Root CA 2021 ===

=== BEGIN HARICA TLS RSA Root CA 2021 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            39:ca:93:1c:ef:43:f3:c6:8e:93:c7:f4:64:89:38:7e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA TLS RSA Root CA 2021
        Validity
            Not Before: Feb 19 10:55:38 2021 GMT
            Not After : Feb 13 10:55:37 2045 GMT
        Subject: C = GR, O = Hellenic Academic and Research Institutions CA, CN = HARICA TLS RSA Root CA 2021
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:8b:c2:e7:af:65:9b:05:67:96:c9:0d:24:b9:d0:
```

```
                0e:64:fc:ce:e2:24:18:2c:84:7f:77:51:cb:04:11:
                36:b8:5e:ed:69:71:a7:9e:e4:25:09:97:67:c1:47:
                c2:cf:91:16:36:62:3d:38:04:e1:51:82:ff:ac:d2:
                b4:69:dd:2e:ec:11:a3:45:ee:6b:6b:3b:4c:bf:8c:
                8d:a4:1e:9d:11:b9:e9:38:f9:7a:0e:0c:98:e2:23:
                1d:d1:4e:63:d4:e7:b8:41:44:fb:6b:af:6b:da:1f:
                d3:c5:91:88:5b:a4:89:92:d1:81:e6:8c:39:58:a0:
                d6:69:43:a9:ad:98:52:58:6e:db:0a:fb:6b:cf:68:
                fa:e3:a4:5e:3a:45:73:98:07:ea:5f:02:72:de:0c:
                a5:b3:9f:ae:a9:1d:b7:1d:b3:fc:8a:59:e7:6e:72:
                65:ad:f5:30:94:23:07:f3:82:16:4b:35:98:9c:53:
                bb:2f:ca:e4:5a:d9:c7:8d:1d:fc:98:99:fb:2c:a4:
                82:6b:f0:2a:1f:8e:0b:5f:71:5c:5c:ae:42:7b:29:
                89:81:cb:03:a3:99:ca:88:9e:0b:40:09:41:33:db:
                e6:58:7a:fd:ae:99:70:c0:5a:0f:d6:13:86:71:2f:
                76:69:fc:90:dd:db:2d:6e:d1:f2:9b:f5:1a:6b:9e:
                6f:15:8c:7a:f0:4b:28:a0:22:38:80:24:6c:36:a4:
                3b:f2:30:91:f3:78:13:cf:c1:3f:35:ab:f1:1d:11:
                23:b5:43:22:9e:01:92:b7:18:02:e5:11:d1:82:db:
                15:00:cc:61:37:c1:2a:7c:9a:e1:d0:ba:b3:50:46:
                ee:82:ac:9d:31:f8:fb:23:e2:03:00:48:70:a3:09:
                26:79:15:53:60:f3:38:5c:ad:38:ea:81:00:63:14:
                b9:33:5e:dd:0b:db:a0:45:07:1a:33:09:f8:4d:b4:
                a7:02:a6:69:f4:c2:59:05:88:65:85:56:ae:4b:cb:
                e0:de:3c:7d:2d:1a:c8:e9:fb:1f:a3:61:4a:d6:2a:
                13:ad:77:4c:1a:18:9b:91:0f:58:d8:06:54:c5:97:
                f8:aa:3f:20:8a:a6:85:a6:77:f6:a6:fc:1c:e2:ee:
                6e:94:33:2a:83:50:84:0a:e5:4f:86:f8:50:45:78:
                00:81:eb:5b:68:e3:26:8d:cc:7b:5c:51:f4:14:2c:
                40:be:1a:60:1d:7a:72:61:1d:1f:63:2d:88:aa:ce:
                a2:45:90:08:fc:6b:be:b3:50:2a:5a:fd:a8:48:18:
                46:d6:90:40:92:90:0a:84:5e:68:31:f8:eb:ed:0d:
                d3:1d:c6:7d:99:18:55:56:27:65:2e:8d:45:c5:24:
                ec:ce:e3
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Subject Key Identifier:
            0A:48:23:A6:60:A4:92:0A:33:EA:93:5B:C5:57:EA:25:4D:BD:12:EE
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
     3e:90:48:aa:6e:62:15:25:66:7b:0c:d5:8c:8b:89:9d:d7:ed:
     4e:07:ef:9c:d0:14:5f:5e:50:bd:68:96:90:a4:14:11:aa:68:
     6d:09:35:39:40:09:da:f4:09:2c:34:a5:7b:59:84:49:29:97:
     74:c8:07:1e:47:6d:f2:ce:1c:50:26:e3:9e:3d:40:53:3f:f7:
```

```
        7f:96:76:10:c5:46:a5:d0:20:4b:50:f4:35:3b:18:f4:55:6a:
        41:1b:47:06:68:3c:bb:09:08:62:d9:5f:55:42:aa:ac:53:85:
        ac:95:56:36:56:ab:e4:05:8c:c5:a8:da:1f:a3:69:bd:53:0f:
        c4:ff:dc:ca:e3:7e:f2:4c:88:86:47:46:1a:f3:00:f5:80:91:
        a2:dc:43:42:94:9b:20:f0:d1:cd:b2:eb:2c:53:c2:53:78:4a:
        4f:04:94:41:9a:8f:27:32:c1:e5:49:19:bf:f1:f2:c2:8b:a8:
        0a:39:31:28:b4:7d:62:36:2c:4d:ec:1f:33:b6:7e:77:6d:7e:
        50:f0:9f:0e:d7:11:8f:cf:18:c5:e3:27:fe:26:ef:05:9d:cf:
        cf:37:c5:d0:7b:da:3b:b0:16:84:0c:3a:93:d6:be:17:db:0f:
        3e:0e:19:78:09:c7:a9:02:72:22:4b:f7:37:76:ba:75:c4:85:
        03:5a:63:d5:b1:75:05:c2:b9:bd:94:ad:8c:15:99:a7:93:7d:
        f6:c5:f3:aa:74:cf:04:85:94:98:00:f4:e2:f9:ca:24:65:bf:
        e0:62:af:c8:c5:fa:b2:c9:9e:56:48:da:79:fd:96:76:15:be:
        a3:8e:56:c4:b3:34:fc:be:47:f4:c1:b4:a8:fc:d5:30:88:68:
        ee:cb:ae:c9:63:c4:76:be:ac:38:18:e1:5e:5c:cf:ae:3a:22:
        51:eb:d1:8b:b3:f3:2b:33:07:54:87:fa:b4:b2:13:7b:ba:53:
        04:62:01:9d:f1:c0:4f:ee:e1:3a:d4:8b:20:10:fa:02:57:e6:
        ef:c1:0b:b7:90:46:9c:19:29:8c:dc:6f:a0:4a:69:69:94:b7:
        24:65:a0:ff:ac:3f:ce:01:fb:21:2e:fd:68:f8:9b:f2:a5:cf:
        31:38:5c:15:aa:e6:97:00:c1:df:5a:a5:a7:39:aa:e9:84:7f:
        3c:51:a8:3a:d9:94:5b:8c:bf:4f:08:71:e5:db:a8:5c:d4:d2:
        a6:fe:00:a3:c6:16:c7:0f:e8:80:ce:1c:28:64:74:19:08:d3:
        42:e3:ce:00:5d:7f:b1:dc:13:b0:e1:05:cb:d1:20:aa:86:74:
        9e:39:e7:91:fd:ff:5b:d6:f7:ad:a6:2f:03:0b:6d:e3:57:54:
        eb:76:53:18:8d:11:98:ba
```

=== END HARICA TLS RSA Root CA 2021 ===

11 ANNEX B (HARICA Common Certificate Profiles)

Friendly Name	Policy IDs	Key Usages	Other Extensions
HARICA CA Certificate	**2.5.29.32.0 (anyPolicy)** or the CP/CPS OID in case of externally operated CA	KU: **Digital Signature, Certificate Signing, CRL Signing** EKU: **Depending on issued Certificate type**	None
OCSP Certificate	**1.3.6.1.4.1.26513.1.1.7**	KU: **Digital Signature** EKU: **OCSP Signing**	**OCSP No Check**
S/MIME Only (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.2.1**	KU: **Digital Signature, Key Encipherment**[8] EKU: **TLS Web Client Authentication, Email Protection**	None
IV Client Authentication Certificate with S/MIME (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.2.3.3**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, Email Protection**	None
OV Client Authentication Certificate with S/MIME (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.2.2.3**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, Email Protection**	None
IV Client Authentication Certificate with S/MIME (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.2.3.1**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, Email Protection, MS Document Signing, AuthenticDocumentsTrust, docSigning**	None

[8] "Key Encipherment" is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

OV Client Authentication Certificate with S/MIME (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.2.2.1**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, Email Protection, MS Document Signing, AuthenticDocumentsTrust**	None
IV Client Authentication Certificate (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.5.1.3**	KU: **Digital Signature** EKU: **TLS Web Client Authentication**	None
OV Client Authentication Certificate (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.5.2.3**	KU: **Digital Signature** EKU: **TLS Web Client Authentication**	None
IV Client Authentication Certificate (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.5.1.1**	KU: **Digital Signature** EKU: **TLS Web Client Authentication**	None
OV Client Authentication Certificate (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.5.2.1**	KU: **Digital Signature** EKU: **TLS Web Client Authentication**	None
Qualified Certificate for Advanced electronic signatures	**0.4.0.194112.1.0 (QCP-n) 1.3.6.1.4.1.26513.1.1.4.1**	KU: **Non Repudiation, Digital Signature, Key Encipherment**[3] (allowed when combined with S/MIME) EKU: **TLS Web Client Authentication, MS Document Signing, AuthenticDocumentsTrust, docSigning**, Email Protection (optional)	**QcStatements:** id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-esign, id-etsi-qcs-SemanticsId-Natural(optional)

Qualified Certificate for Qualified electronic signatures	**0.4.0.194112.1.2 (QCP-n-qscd)** **1.3.6.1.4.1.26513.1.1.4.2**	KU: **Non Repudiation, Digital Signature** EKU: **TLS Web Client Authentication, MS Document Signing, AuthenticDocumentsTrust, docSigning**, **Smartcard Logon**, Email Protection (optional)	**QcStatements:** id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, id-etsi-qcs-QcPDS, id-etsi-qct-esign, id-etsi-qcs-SemanticsId-Natural (optional) **SmartcardUser** (optional)
Qualified Certificate for Advanced electronic seal	**0.4.0.194112.1.1 (QCP-l)** **1.3.6.1.4.1.26513.1.1.4.3**	KU: **Non Repudiation, Digital Signature, Key Encipherment**[3] (allowed when combined with S/MIME) EKU: **TLS Web Client Authentication, MS Document Signing, AuthenticDocumentsTrust, docSigning**, Email Protection (optional)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(optional), id-etsi-psd2-qcStatement (optional)
Qualified Certificate for Qualified electronic seal	**0.4.0.194112.1.3 (QCP-l-qscd)** **1.3.6.1.4.1.26513.1.1.4.4**	KU: **Non Repudiation, Digital Signature** EKU: **TLS Web Client Authentication, MS Document Signing, AuthenticDocumentsTrust, docSigning**, Email Protection (optional)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(optional), id-etsi-psd2-qcStatement (optional)
Qualified Certificate for PSD2 Advanced electronic seal	**0.4.0.194112.1.3 (QCP-l-qscd)** **1.3.6.1.4.1.26513.1.1.4.5 (QCP-l-psd2)**	KU: **Non Repudiation, Digital Signature** EKU: **TLS Web Client Authentication, MS Document Signing, AuthenticDocumentsTrust, docSigning**, Email Protection (optional)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(optional), id-etsi-psd2-qcStatement

Qualified Certificate for PSD2 Qualified electronic seal	**0.4.0.194112.1.3 (QCP-l-qscd)** **1.3.6.1.4.1.26513.1.1.4.6 (QCP-l-psd2-qscd)**	KU: **Non Repudiation, Digital Signature** EKU: **TLS Web Client Authentication, MS Document Signing, AuthenticDocumentsTrust, docSigning**, Email Protection (optional)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(optional), id-etsi-psd2-qcStatement
Qualified Certificate for Website Authentication for Legal Entity (Organization Validation)	**0.4.0.194112.1.4 (QNCP-w-OV),** **2.23.140.1.2.2,** **1.3.6.1.4.1.26513.1.1.1.7**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-web, id-etsi-qcs-SemanticsId-Legal(optional)
Qualified Certificate for Website Authentication for Natural Person	**0.4.0.194112.1.4 (QNCP-w-IV),** **2.23.140.1.2.3,** **1.3.6.1.4.1.26513.1.1.1.8**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-web, id-etsi-qcs-SemanticsId-Legal(optional)
Qualified Certificate for Website Authentication for Legal Entity (Extended Validation)	**0.4.0.194112.1.4 (QEVCP-w),** **2.23.140.1.1,** **1.3.6.1.4.1.26513.1.1.1.5**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-web, id-etsi-qcs-SemanticsId-Legal(optional) **cabfOrganizationIdentifier** (optional)

Qualified Certificate for PSD2 Website Authentication outside the context of a web browser	**0.4.0.19495.3.1 (QCP-w-psd2), 0.4.0.194112.1.6 (QNCP-w-gen), 1.3.6.1.4.1.26513.1.1.1.9**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-web, id-etsi-qcs-SemanticsId-Legal(optional), id-etsi-psd2-qcStatement
Qualified Certificate for PSD2 Website Authentication	**0.4.0.19495.3.1 (QEVCP-w-psd2), 2.23.140.1.1, 1.3.6.1.4.1.26513.1.1.1.6**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-web, id-etsi-qcs-SemanticsId-Legal(optional), id-etsi-psd2-qcStatement
Time stamping	**0.4.0.2023.1.1 (BTSP), 1.3.6.1.4.1.26513.1.1.6.1**	KU: **Digital Signature** EKU:**Time Stamping**	None
Time stamping for Code Signing	**2.23.140.1.4.2, 1.3.6.1.4.1.26513.1.1.6.3**	KU: **Digital Signature** EKU:**Time Stamping**	None
Qualified Time stamping	**0.4.0.2023.1.1 (BTSP), 1.3.6.1.4.1.26513.1.1.6.2**	KU: **Non Repudiation, Digital Signature** EKU:**Time Stamping**	None
IV Code Signing Certificate in Secure Signature Creation Device	**0.4.0.2042.1.2 (NCP+), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.2.2**	KU: **Digital Signature** EKU:**Code Signing**, Lifetime Signing (optional)	None
OV Code Signing Certificate in Secure Signature Creation Device	**0.4.0.2042.1.2 (NCP+), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.1.2**	KU: **Digital Signature** EKU:**Code Signing**, Lifetime Signing (optional)	None

EV Code Signing Certificate	**0.4.0.2042.1.2 (NCP+), 2.23.140.1.3, 1.3.6.1.4.1.26513.1.3.3**	KU: **Digital Signature** EKU:**Code Signing**, Lifetime Signing (optional)	None
DV SSL/TLS Certificate	**0.4.0.2042.1.6 (DVCP), 2.23.140.1.2.1, 1.3.6.1.4.1.26513.1.1.1.1**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None
OV SSL/TLS Certificate	**0.4.0.2042.1.7 (OVCP), 2.23.140.1.2.2, 1.3.6.1.4.1.26513.1.1.1.2**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None
IV SSL/TLS Certificate	**0.4.0.2042.1.8 (IVCP), 2.23.140.1.2.3, 1.3.6.1.4.1.26513.1.1.1.3**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None
EV SSL/TLS Certificate	**0.4.0.2042.1.4 (EVCP), 2.23.140.1.1, 1.3.6.1.4.1.26513.1.1.1.4**	KU: **Digital Signature, Key Encipherment**[3] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None

12 ANNEX C (HARICA Hierarchy)

HARICA “Unconstrained” and “Technically Constrained” Subordinate CAs, per section 7.1.5 are available on https://repo.harica.gr.

13 Annex D CAA Contact Tag

These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.

13.1 CAA Methods

13.1.1 CAA contactemail Property

SYNTAX: `contactemail` <rfc6532emailaddress>

The CAA `contactemail` property takes an email address as its parameter. The entire parameter value SHALL be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.

The following is an example where the holder of the domain specified the contact property using an email address.

```
$ORIGIN example.com.

     CAA 0 contactemail "domainowner@example.com"
```

The `contactemail` property MAY be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

13.1.2 CAA contactphone Property

SYNTAX: contactphone <rfc3966 Global Number>

The CAA `contactphone` property takes a phone number as its parameter. The entire parameter value SHALL be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used. Global Numbers SHALL have a preceding + and a country code and MAY contain spaces as visual separators.

The following is an example where the holder of the domain specified the contact property using a phone number.

```
$ORIGIN example.com.

     CAA 0 contactphone "+1 (555) 123-4567"
```

The `contactphone` property MAY be critical if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

13.2 DNS TXT Methods

13.2.1 DNS TXT Record Email Contact

The DNS TXT record SHALL be placed on the "`_validation-contactemail`" subdomain of the domain being validated. The entire RDATA value of this TXT record SHALL be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.

13.2.2 DNS TXT Record Phone Contact

The DNS TXT record SHALL be placed on the "`_validation-contactphone`" subdomain of the domain being validated. The entire RDATA value of this TXT record SHALL be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used.

14 ANNEX E Issuance of Certificates for Onion Domain Names

This appendix defines permissible verification procedures for including one or more Onion Domain Names in a Certificate.

1. The Domain Name SHALL contain at least two Domain Labels, where the rightmost Domain Label is "onion", and the Domain Label immediately preceding the rightmost "onion" Domain Label is a valid Version 3 Onion Address, as defined in section 6 of the Tor Rendezvous Specification - Version 3 located at https://spec.torproject.org/rend-spec-v3.
2. HARICA SHALL verify the Applicant's control over the Onion Domain Name using at least one of the methods listed below:
    a. by using Domain Validation method 3.2.2.4.18 or 3.2.2.4.19. When these methods are used to verify the Applicant's control over the .onion service, HARICA SHALL use Tor protocol to establish a connection to the .onion hidden service. HARICA SHALL NOT delegate or rely on a third-party to establish the connection, such as by using Tor2Web; or
    b. by having the Applicant provide a Certificate Request signed using the .onion service's private key, if the Attributes section of the `certificationRequestInfo` contains:
        i. A `caSigningNonce` attribute that contains a Random Value that is generated by HARICA; and
        ii. An `applicantSigningNonce` attribute that contains a single value. HARICA SHALL recommend to Applicants that the `applicantSigningNonce` value should contain at least 64 bits of entropy.

    The signing nonce attributes have the following format:

```
ASN.1
cabf    OBJECT    IDENTIFIER    ::=    {    joint-iso-itu-t(2)
international-organizations(23) ca-browser-forum(140) }

caSigningNonce ATTRIBUTE ::= {

| WITH SYNTAX | OCTET STRING |
| --- | --- |
| EQUALITY MATCHING RULE | octetStringMatch |
| SINGLE VALUE | TRUE |
| ID | { cabf-caSigningNonce } |

}

cabf-caSigningNonce OBJECT IDENTIFIER ::= { cabf 41 }

applicantSigningNonce ATTRIBUTE ::= {

| WITH SYNTAX | OCTET STRING |
| --- | --- |
| EQUALITY MATCHING RULE | octetStringMatch |
| SINGLE VALUE | TRUE |
| ID | { cabf-applicantSigningNonce } |
```

```
}

cabf-applicantSigningNonce OBJECT IDENTIFIER ::= { cabf 42 }
```

This method is suitable for validating Wildcard Onion Domain Names.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

HARICA MAY include a wildcard character in the Subject Alternative Name Extension and Subject Common Name Field as the left-most character in the Onion Domain Name provided inclusion of the wildcard character complies with section 3.2.2.6.

3. When a Certificate includes an Onion Domain Name, the Domain Name shall not be considered an Internal Name provided that the Certificate was issued in compliance with this Annex.

15 ANNEX F HARICA Policy Identifiers

HARICA has been assigned a private enterprise number from IANA with ID **26513** https://oidref.com/1.3.6.1.4.1.26513 .

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 26513(26513)}

This is the full list of custom HARICA Policy OIDs for each certificate type, including compatibility with other internationally recognized policy OIDS of various standards.

OID	Description
1.3.6.1.4.1.26513	
.1	Certification Services Provision
.1.0	Central Certificate Policy/Certification Practice Statement
.1.0.3	First digit of the version number of the Central Certificate Policy/Certification Practice Statement
.1.0.8	Second digit of the version number of the Central Certificate Policy/Certification Practice Statement
.1.1	Certificate Policy for specific certificate type
.1.1.1	**Server Authentication**
.1.1.1.1	Domain Validation (DV) compatible with - CA/B Forum OID 2.23.140.1.2.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.6
.1.1.1.2	Organization Validation (OV) compatible with - CA/B Forum OID 2.23.140.1.2.2 - ETSI EN 319 411-1 OID 0.4.0.2042.1.7
.1.1.1.3	Individual Validation (IV) compatible with - CA/B Forum OID 2.23.140.1.2.3 - ETSI EN 319 411-1 OID 0.4.0.2042.1.8
.1.1.1.4	Extended Validation (EV) compatible with - CA/B Forum OID 2.23.140.1.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.4
.1.1.1.5	Qualified Website Authentication (QEVCP-w) compatible with - CA/B Forum OID 2.23.140.1.1 - ETSI EN 319 411-2 OID 0.4.0.194112.1.4 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
.1.1.1.6	Qualified Website Authentication for PSD2 (QCP-w-psd2) compatible with - ETSI TS 119 495 OID 0.4.0.19495.3.1 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024 - Directive (EU) 2015/2366
.1.1.1.7	Qualified Website Authentication (QNCP-w-OV) compatible with - CA/B Forum OID 2.23.140.1.2.2 - ETSI EN 319 411-2 OID 0.4.0.194112.1.5 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
.1.1.1.8	Qualified Website Authentication (QNCP-w-IV) compatible with - CA/B Forum OID 2.23.140.1.2.3

							- ETSI EN 319 411-2 OID 0.4.0.194112.1.5 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
				9			Qualified Website Authentication (QNCP-w-gen) compatible with - ETSI EN 319 411-2 OID 0.4.0.194112.1.6 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
			2				**Email Signing**
				1			Simple Email Validation (LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
					1		Simple Email Validation (LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3 and - CA/B Forum OID 2.23.140.1.5.1.1 mailbox-validated (1) legacy (1)
					2		Simple Email Validation (LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3 and - CA/B Forum OID 2.23.140.1.5.1.2 mailbox-validated (1) multipurpose (2)
					3		Simple Email Validation (LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3 and - CA/B Forum OID 2.23.140.1.5.1.3 mailbox-validated (1) strict (3)
				2			Organization Validation (OV)
					1		Organization Validation (OV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.2.1 organization-validated (2) legacy (1)
					2		Organization Validation (OV-NCP+) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.2 and - CA/B Forum OID 2.23.140.1.5.2.1 organization-validated (2) legacy (1)
					3		Organization Validation (OV-LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
					4		Organization Validation (OV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.2.2 organization-validated (2) multipurpose (2)
					5		Organization Validation (OV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.2.3 organization-validated (2) strict (3)
				3			Individual Validation (IV)
					1		Individual Validation (IV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.4.1 individual-validated (4) legacy (1)
					2		Individual Validation (IV-NCP+) compatible with - ETSI EN 319 411-1 0.4.0.2042.1.2
					3		Individual Validation (IV-LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
					4		Individual Validation (IV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.4.2 individual-validated (4) multipurpose (2)
					5		Individual Validation (IV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.4.3 individual-validated (4) strict (3)

			4			Sponsored Validation (SV)
				1		Sponsored Validation (SV-LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3 and - CA/B Forum OID 2.23.140.1.5.3.1 sponsor-validated (3) legacy (1)
				2		Sponsored Validation (SV-LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3 and - CA/B Forum OID 2.23.140.1.5.3.2 sponsor-validated (3) multipurpose (2)
				3		Sponsored Validation (SV-LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3 and - CA/B Forum OID 2.23.140.1.5.3.3 sponsor-validated (3) strict (3)
				4		Sponsored Validation (SV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.3.1 sponsor-validated (3) legacy (1)
				5		Sponsored Validation (SV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.3.2 sponsor-validated (3) multipurpose (2)
				6		Sponsored Validation (SV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1 and - CA/B Forum OID 2.23.140.1.5.3.3 sponsor-validated (3) strict (3)
		3				**Code Signing**
			1			Organization Validation (OV)
				1		Organization Validation (OV-NCP) compatible with - CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
				2		Organization Validation (OV-NCP+) compatible with - CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
			2			Individual Validation (IV)
				1		Individual Validation (IV-NCP) compatible with - CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
				2		Individual Validation (IV-NCP+) compatible with - CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
				3		Extended Validation (EV) compatible with - CA/B Forum OID 2.23.140.1.3 - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
		4				**Document Signing**
			1			Qualified Certificates for Advanced Electronic Signatures (QCP-n) compatible with - ETSI EN 319 411-2 OID 0.4.0.194112.1.0 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
			2			Qualified Certificates for Qualified Electronic Signatures (QCP-n-qscd) compatible - ETSI EN 319 411-2 OID 0.4.0.194112.1.2 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
			3			Qualified Certificates for Advanced Electronic Seals (QCP-l) compatible with - ETSI EN 319 411-2 OID 0.4.0.194112.1.1

						- Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
				4		Qualified Certificates for Qualified Electronic Seals (QCP-l-qscd) compatible with - ETSI EN 319 411-2 OID 0.4.0.194112.1.3 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
				5		Qualified Certificates for PSD2 Advanced Electronic Seals (QCP-l-psd2) compatible with - ETSI EN 319 411-2 OID 0.4.0.194112.1.1 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024 - Directive (EU) 2015/2366
				6		Qualified Certificates for PSD2 Qualified Electronic Seals (QCP-l-psd2-qscd) compatible with - ETSI EN 319 411-2 OID 0.4.0.194112.1.3 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024 - Directive (EU) 2015/2366
			5			**Client Authentication**
				1		Individual Validation (IV)
					1	Individual Validation (IV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
					2	Individual Validation (IV-NCP+) compatible with - ETSI EN 319 411-1 0.4.0.2042.1.2
					3	Individual Validation (IV-LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
				2		Organization Validation (OV)
					1	Organization Validation (OV-NCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
					2	Organization Validation (OV-NCP+) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
					3	Organization Validation (OV-LCP) compatible with - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
			6			**Time Stamping**
				1		Simple Time Stamping (BTST) compatible with - ETSI EN 319 421 OID 0.4.0.2023.1.1
				2		Qualified Time Stamping (QTST) compatible with - ETSI EN 319 421 OID 0.4.0.2023.1.1 - Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024
				3		Time Stamping for Code Signing compatible with CA/B Forum OID 2.23.140.1.4.2
			7			**OCSP Responder Certificate**
			8			**Remote QSCD**