

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 4.2 (September 30th 2020)

Table of Contents

1	INTRODUCTION	6
1.1	OVERVIEW	6
1.2	DOCUMENT NAME AND IDENTIFICATION	7
1.3	PKI PARTICIPANTS	8
1.3.1	<i>Certification Authorities</i>	8
1.3.2	<i>Registration Authorities</i>	8
1.3.3	<i>Subscribers</i>	9
1.3.4	<i>Relying Parties</i>	9
1.3.5	<i>Other participants</i>	10
1.4	CERTIFICATE USAGE	10
1.4.1	<i>Appropriate certificate uses</i>	10
1.4.2	<i>Forbidden certificate use</i>	11
1.5	POLICY ADMINISTRATION	11
1.5.1	<i>Policy Making Organization</i>	11
1.5.2	<i>Contact persons</i>	11
1.5.3	<i>Policy enforcement persons</i>	12
1.5.4	<i>CPS approval procedures</i>	12
1.6	DEFINITIONS AND ACRONYMS	12
1.6.1	<i>Definitions</i>	12
1.6.2	<i>Acronyms</i>	25
2	PUBLICATION AND REPOSITORY	27
2.1	REPOSITORIES	27
2.2	DISCLOSURE OF CERTIFICATION AUTHORITY INFORMATION	27
2.3	FREQUENCY OF PUBLICATION	27
2.4	ACCESS CONTROLS ON REPOSITORIES	27
3	IDENTIFICATION AND AUTHENTICATION	28
3.1	NAMING	28
3.1.1	<i>Type of Names</i>	28
3.1.1.1	<i>Certificate name compliance with Baseline Requirements</i>	28
3.1.2	<i>Obligation for meaningful names</i>	28
3.1.3	<i>Anonymity or pseudonymity of subscribers</i>	28
3.1.4	<i>Rules for interpreting various name forms</i>	28
3.1.4.1	<i>End-Entity Certificates for electronic signatures</i>	29
3.1.4.2	<i>End-Entity Certificates for electronic seals</i>	30
3.1.4.3	<i>End-Entity Certificates for SSL/TLS usage</i>	30
3.1.4.4	<i>End-Entity Certificates for Code Signing</i>	30
3.1.4.5	<i>End-Entity Certificates for Web Client Authentication</i>	31
3.1.5	<i>Uniqueness of names</i>	31
3.1.6	<i>Resolution Process regarding disputes about naming property rights and the role of trademarks</i>	31
3.2	INITIAL IDENTITY VALIDATION	32
3.2.1	<i>Method to prove possession of private key</i>	32
3.2.2	<i>Authentication of organization identity</i>	32
3.2.2.1	<i>Identity</i>	33
3.2.2.2	<i>DBA/Tradename/Roles</i>	33
3.2.2.3	<i>Verification of Country</i>	34
3.2.2.4	<i>Validation of Domain Authorization or Control</i>	34
3.2.2.5	<i>Authentication for an IP Address</i>	41
3.2.2.6	<i>Wildcard Domain Validation</i>	43
3.2.2.7	<i>Data Source Accuracy</i>	43
3.2.2.8	<i>CAA Records</i>	45

3.2.3	<i>Authentication of individual person identity</i>	45
3.2.3.1	Entity applying for a user certificate.....	46
3.2.3.2	Individual who applies for a device certificate	48
3.2.4	<i>Non verified subscriber information</i>	48
3.2.5	<i>Validation of Authority</i>	48
3.2.6	<i>Criteria for interoperability</i>	49
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	49
3.3.1	<i>Identification and authentication for routine re-key</i>	49
3.3.2	<i>Identification and authentication for re-key after revocation</i>	49
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS	49
3.4.1	<i>Revocation request from Issuing Authority</i>	49
3.4.2	<i>Revocation request from Subscriber</i>	50
3.4.3	<i>Revocation request from non-Subscriber</i>	50
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	51
4.1	CERTIFICATE APPLICATION.....	51
4.1.1	<i>Who is eligible to submit a certificate request</i>	51
4.1.2	<i>Enrollment process and responsibilities</i>	51
4.1.2.1	Enrollment process for EV Certificates	51
4.2	CERTIFICATE APPLICATION PROCESSING	52
4.2.1	<i>Subscriber identification and authentication procedures</i>	52
4.2.2	<i>Approval or rejection of certificate applications</i>	53
4.2.3	<i>Time to process certificate applications</i>	53
4.2.4	<i>Certificate Authority Authorization (CAA)</i>	54
4.3	CERTIFICATE ISSUANCE	54
4.3.1	<i>CA Actions during Certificate issuance</i>	54
4.3.2	<i>Notification to Subscribers by the CA regarding issuance of certificate</i>	54
4.4	CERTIFICATE ACCEPTANCE.....	54
4.4.1	<i>Conduct constituting certificate acceptance</i>	54
4.4.2	<i>Publication of the certificate by the CA</i>	54
4.4.3	<i>Notification of other entities about certificate issuance by the CA</i>	55
4.5	KEY PAIR AND CERTIFICATE USAGE.....	55
4.5.1	<i>Subscriber private key and certificate usage</i>	55
4.5.2	<i>Relying party public key and certificate usage</i>	55
4.6	CERTIFICATE RENEWAL	55
4.6.1	<i>Prerequisite Circumstances for certificate renewal</i>	55
4.6.2	<i>Who may request renewal</i>	55
4.6.3	<i>Processing certificate renewal requests</i>	55
4.6.4	<i>Notification of new certificate issuance to Subscriber</i>	56
4.6.5	<i>Conduct constituting acceptance of a renewal certificate</i>	56
4.6.6	<i>Publication of the renewal certificate by the CA</i>	56
4.6.7	<i>Notification of certificate issuance by the CA to other entities</i>	56
4.7	CERTIFICATE RE-KEYING	56
4.7.1	<i>Circumstance for certificate re-keying</i>	56
4.7.2	<i>Who may request certification of a new public key</i>	56
4.7.3	<i>Processing certificate re-keying requests</i>	56
4.7.4	<i>Notification of new re-keyed certificate issuance to Subscriber</i>	56
4.7.5	<i>Conduct constituting acceptance of a re-keyed certificate</i>	56
4.7.6	<i>Publication of the re-keyed certificate by the CA</i>	56
4.7.7	<i>Notification of re-keyed certificate issuance by the CA to other entities</i>	57
4.8	CERTIFICATE MODIFICATION	57
4.8.1	<i>Circumstance for certificate modification</i>	57
4.8.2	<i>Who may request certificate modification</i>	57
4.8.3	<i>Processing certificate modification requests</i>	57
4.8.4	<i>Notification of new certificate issuance to Subscriber</i>	57
4.8.5	<i>Conduct constituting acceptance of the certificate</i>	57

4.8.6	<i>Publication of the modified certificate by the CA</i>	57
4.8.7	<i>Notification of certificate issuance by the CA to other entities</i>	57
4.9	CERTIFICATE REVOCATION AND SUSPENSION	57
4.9.1	<i>Circumstances for revocation</i>	57
4.9.1.1	Reasons for Revoking a Subscriber Certificate	57
4.9.1.2	Reasons for Revoking a Subordinate CA Certificate.....	59
4.9.2	<i>Who can request a revocation</i>	60
4.9.3	<i>Procedure for revocation request</i>	60
4.9.3.1	Certificate revocation by the Subscriber.....	60
4.9.3.2	Certificate revocation by any other entity.....	60
4.9.3.3	Revocation request by an Application Software Supplier.....	61
4.9.3.4	Revocation request by the eIDAS National Supervisory Body.....	61
4.9.3.5	Revocation request by a National Competent Authority.....	61
4.9.4	<i>Revocation request grace period</i>	62
4.9.4.1	Certificates used for “Signing” revocation dates	62
4.9.5	<i>Time within which CA must process the revocation request</i>	63
4.9.6	<i>Revocation checking requirement for relying parties</i>	63
4.9.7	<i>CRL issuance frequency</i>	63
4.9.8	<i>Maximum latency for CRLs</i>	64
4.9.9	<i>Online revocation/status checking availability (OCSP)</i>	64
4.9.10	<i>Online revocation checking requirements</i>	64
4.9.11	<i>Other forms of revocation advertisements available</i>	65
4.9.12	<i>Special requirements re-key compromise</i>	66
4.9.13	<i>Circumstances for suspension</i>	66
4.9.14	<i>Who can request suspension</i>	66
4.9.15	<i>Procedure for suspension request</i>	66
4.9.16	<i>Limits on suspension period</i>	66
4.10	CERTIFICATE STATUS SERVICES	66
4.10.1	<i>Operational characteristics</i>	66
4.10.1.1	Online Certificate status service OCSP	67
4.10.1.2	Online Certificate Repository	67
4.10.1.3	Usage of Certificate Revocation Lists (CRL)	67
4.10.2	<i>Service Availability</i>	67
4.10.3	<i>Optional features</i>	67
4.11	END OF SUBSCRIPTION	67
4.12	KEY ESCROW AND RECOVERY	67
4.12.1	<i>Key escrow and recovery policy and practices</i>	67
4.12.2	<i>Session key encapsulation and recovery policy and practices</i>	67
5	ADMINISTRATIVE, TECHNICAL AND OPERATIONAL CONTROLS	68
5.1	PHYSICAL SECURITY AND ACCESS CONTROLS	68
5.1.1	<i>Site location</i>	68
5.1.2	<i>Physical access</i>	68
5.1.3	<i>Power and cooling</i>	68
5.1.4	<i>Water exposures</i>	68
5.1.5	<i>Fire prevention and protection</i>	68
5.1.6	<i>Media storage</i>	68
5.1.7	<i>Waste Disposal</i>	69
5.1.8	<i>Off-site backup</i>	69
5.2	PROCEDURAL CONTROLS	69
5.2.1	<i>Trusted roles</i>	69
5.2.2	<i>Number of persons required per task</i>	69
5.2.3	<i>Identification and authentication for each role</i>	69
5.2.4	<i>Roles requiring separation of duties</i>	69
5.3	PERSONNEL CONTROLS	70
5.3.1	<i>Qualifications, experience and clearance requirements</i>	70
5.3.2	<i>Background check procedures</i>	70

5.3.3	Training requirements.....	70
5.3.4	Re-training frequency and requirements.....	70
5.3.5	Job rotation frequency and sequence.....	70
5.3.6	Sanctions for unauthorized actions.....	70
5.3.7	Independent contractor's requirements working outside GUnet and involved with the HARICA PKI.....	70
5.3.8	Documentation supplied to the personnel.....	71
5.4	AUDIT LOGGING PROCEDURES.....	71
5.4.1	Types of events recorded.....	71
5.4.2	Frequency of processing log.....	72
5.4.3	Retention period for audit log.....	72
5.4.4	Protection of audit log.....	72
5.4.5	Audit log backup procedures.....	72
5.4.6	Audit collection system (internal vs. external).....	72
5.4.7	Notification to event-causing subject.....	72
5.4.8	Vulnerability assessments.....	72
5.5	RECORDS ARCHIVAL.....	73
5.5.1	Types of records archived.....	73
5.5.2	Retention period for archive.....	73
5.5.3	Protection of archive.....	73
5.5.3.1	Access.....	73
5.5.3.2	Protection against the alteration of the records file.....	73
5.5.3.3	Protection against the deletion of the records file.....	73
5.5.3.4	Protection against the deterioration of storage media.....	74
5.5.3.5	Protection against future lack of availability of readers of the old media.....	74
5.5.4	Archive backup procedures.....	74
5.5.5	Requirements for time-stamping of records.....	74
5.5.6	Archive collection system (internal or external).....	74
5.5.7	Procedures to obtain and verify archive information.....	74
5.6	KEY CHANGEOVER.....	74
5.7	COMPROMISE AND DISASTER RECOVERY.....	74
5.7.1	Incident and compromise handling procedures.....	74
5.7.2	Computing resources, software and/or data are corrupted.....	75
5.7.3	Private key compromise procedures.....	75
5.7.4	Business continuity capabilities after a disaster.....	75
5.8	CERTIFICATION AUTHORITY OR REGISTRATION AUTHORITY TERMINATION.....	76
6	TECHNICAL SECURITY CONTROLS.....	77
6.1	KEY PAIR GENERATION AND INSTALLATION.....	77
6.1.1	Key pair generation.....	77
6.1.1.1	CA and TSU Key Pair Generation.....	77
6.1.1.2	RA Key Pair Generation.....	77
6.1.1.3	Subscriber Key Pair Generation.....	77
6.1.2	Private Key delivery to Subscriber.....	78
6.1.3	Public key delivery to certificate issuer.....	79
6.1.4	CA public key delivery to relying parties.....	79
6.1.5	Key sizes.....	79
6.1.6	Public key generation parameters and quality checking.....	80
6.1.7	Key usage purposes as per X.509v3 key usage field.....	80
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING	80
CONTROLS		
6.2.1	Cryptographic module standards and controls.....	80
6.2.2	Private Key control from multiple persons (N out of M).....	81
6.2.3	Private Key escrow.....	81
6.2.4	Private Key backup.....	82
6.2.5	Private Key archival.....	82
6.2.6	Private Key transfer into or from a cryptographic module.....	82

6.2.7	<i>Private Key storage on cryptographic module</i>	82
6.2.8	<i>Methods of activating private key</i>	82
6.2.8.1	Who can activate (use) a private key	82
6.2.8.2	Actions to be performed to activate a private key.....	83
6.2.8.3	Once activated, for how long is the key «active»?.....	83
6.2.9	<i>Methods for deactivating private key</i>	83
6.2.10	<i>Methods for destroying private key</i>	83
6.2.11	<i>Cryptographic module rating</i>	83
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	84
6.3.1	<i>Public key archival</i>	84
6.3.2	<i>Certificate operational periods and key pair usage periods</i>	84
6.4	ACTIVATION DATA.....	84
6.4.1	<i>Activation data generation and installation</i>	84
6.4.2	<i>Activation data protection</i>	84
6.4.3	<i>Other aspects of activation data</i>	85
6.5	COMPUTER SECURITY CONTROLS	85
6.5.1	<i>Specific computer security technical requirements</i>	85
6.5.2	<i>Computer security rating</i>	85
6.6	LIFE CYCLE TECHNICAL CONTROLS.....	85
6.6.1	<i>System development controls</i>	85
6.6.2	<i>Security management controls</i>	85
6.6.3	<i>Life cycle security controls</i>	85
6.7	NETWORK SECURITY CONTROLS	85
6.8	TIME-STAMPING.....	86
6.8.1	<i>Time-Stamp Issuance</i>	86
6.8.2	<i>Time-Stamping Unit</i>	86
6.8.3	<i>Time-Stamp Token</i>	86
6.8.4	<i>Clock synchronization with UTC</i>	87
7	CERTIFICATE, CRL AND OCSP PROFILES	87
7.1	CERTIFICATE PROFILE	87
7.1.1	<i>Version number</i>	87
7.1.2	<i>Certificate extensions</i>	87
7.1.3	<i>Algorithm Object Identifiers</i>	89
7.1.3.1	SubjectPublicKeyInfo.....	89
7.1.3.2	Signature AlgorithmIdentifier.....	90
7.1.4	<i>Name Forms</i>	92
7.1.4.1	Serial number.....	92
7.1.4.2	Signature Algorithm	92
7.1.4.3	Signature.....	92
7.1.4.4	Issuer	92
7.1.4.6	Valid To.....	93
7.1.4.7	Subject Information	93
7.1.4.8	Subject Alternative Name Extension	96
7.1.5	<i>Name constraints</i>	97
7.1.6	<i>Certificate policy object identifier</i>	98
7.1.7	<i>Usage of Policy Constraints extension</i>	100
7.1.8	<i>Policy qualifiers syntax and semantics</i>	100
7.1.9	<i>Processing semantics for the critical Certificate Policies extension</i>	100
7.2	CRL PROFILE.....	100
7.2.1	<i>Version number(s)</i>	100
7.2.2	<i>CRL and CRL entry extensions</i>	100
7.2.2.1	Signature.....	100
7.2.2.2	Hashing Algorithm	101
7.2.2.3	Issuer Name	101
7.2.2.4	This Update	101
7.2.2.5	Next Update.....	101
7.2.2.6	Revoked Certificates.....	101

7.2.2.7	CRL Number (OID 2.5.29.20).....	101
7.2.2.8	Authority Key Identifier	101
7.2.2.9	Expired certificates on CRL (OID: 2.5.29.60).....	101
7.2.2.10	Reason Code (OID 2.5.29.21)	101
7.3	OCSP PROFILE	102
7.3.1	Version number	102
7.3.2	OCSP extensions	102
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	102
8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	103
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR.....	103
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	103
8.4	TOPICS COVERED BY ASSESSMENT	103
8.5	ACTIONS TAKEN BECAUSE OF DEFICIENCY	104
8.6	COMMUNICATION OF RESULTS	104
8.7	SELF-AUDITS	104
9	OTHER BUSINESS AND LEGAL MATTERS	105
9.1	FEES.....	105
9.1.1	Certificate issuance or renewal fees.....	105
9.1.2	Certificate access fees	105
9.1.3	Revocation or status information access fees.....	105
9.1.4	Fees for other services	105
9.1.5	Refund policy.....	105
9.2	FINANCIAL RESPONSIBILITY	105
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION.....	105
9.3.1	Scope of confidential information	105
9.3.2	Information not within the scope of confidential information	105
9.3.3	Responsibility to protect confidential information	106
9.4	PRIVACY OF PERSONAL INFORMATION	106
9.4.1	Privacy plan	106
9.4.2	Information treated as private.....	106
9.4.3	Information not deemed private	106
9.4.4	Responsibility to protect private information.....	106
9.4.5	Notice and consent to use private information.....	106
9.4.6	Disclosure pursuant to judicial or administrative process.....	107
9.4.7	Other information disclosure circumstances.....	107
9.5	INTELLECTUAL PROPERTY RIGHTS	107
9.6	REPRESENTATIONS AND WARRANTIES	107
9.6.1	CA Representations and Warranties	107
9.6.1.1	Responsibilities of externally-operated Certification Authorities	109
9.6.2	RA Representations and Warranties.....	110
9.6.3	Subscriber Representations and Warranties	111
9.6.4	Relying Party Representations and Warranties	112
9.6.5	Representations and Warranties of Other Participants	113
9.7	DISCLAIMERS OF WARRANTIES	113
9.8	LIMITATIONS OF LIABILITY	113
9.9	INDEMNIFICATION.....	114
9.10	TERM AND TERMINATION	114
9.10.1	Term and termination for Subscriber Agreements	114
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS	115
9.12	AMENDMENTS.....	115
9.12.1	Procedure for amendment.....	115
9.12.2	Notification mechanism and period.....	115
9.12.3	Circumstances under which OID must be changed.....	115
9.13	DISPUTE RESOLUTION PROVISIONS.....	116

9.14	GOVERNING LAW	116
9.15	COMPLIANCE WITH APPLICABLE LAW	116
9.16	MISCELLANEOUS PROVISIONS	116
9.16.1	<i>Entire Agreement</i>	116
9.16.2	<i>Assignment</i>	116
9.16.3	<i>Severability</i>	116
9.16.4	<i>Enforcement</i>	117
9.16.5	<i>Force Majeure</i>	117
9.17	OTHER PROVISIONS	117
10	ANNEX A (HARICA ROOTS)	118
11	ANNEX B (HARICA COMMON CERTIFICATE PROFILES).....	123
12	ANNEX C (HARICA HIERARCHY).....	128
12.1	UNCONSTRAINED SUBORDINATE CAS	128
12.2	TECHNICALLY CONSTRAINED SUBORDINATE CAS	128
13	ANNEX D CAA CONTACT TAG	130
13.1	CAA METHODS	131
13.1.1	<i>CAA contactemail Property</i>	131
13.1.2	<i>CAA contactphone Property</i>	131
13.2	DNS TXT METHODS	131
13.2.1	<i>DNS TXT Record Email Contact</i>	131
13.2.2	<i>DNS TXT Record Phone Contact</i>	132
14	ANNEX E ISSUANCE OF CERTIFICATES FOR .ONION DOMAIN NAMES	133
15	ANNEX F HARICA POLICY IDENTIFIERS	135

Version control

Version	Date	Comment
2.2	March 2011	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Adding NameConstraints
2.6	Apr 2012	<ul style="list-style-type: none"> • CodeSigning Certificates • Certificate store functionality
2.7	Apr 2013	<ul style="list-style-type: none"> • Incorporate CA/B Forum BR for Publicly-Trusted Certificates 1.1 • CRL, OCSP nextUpdate fields
3.0	Dec 2014	<ul style="list-style-type: none"> • Incorporate CA/B Forum BR for Publicly-Trusted Certificates 1.1.9 • Incorporate Microsoft Root Certificate Program –Technical Requirements 2.0

		<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Adding qualified certificate extensions (qcStatements)
3.2	June 2015	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Refine language regarding the term “CA”, “TSP” • Added scope for cross-signing
3.5	May 2017	<ul style="list-style-type: none"> • 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)

		<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

		<ul style="list-style-type: none"> • Incorporate CA/B Forum EV Code Signing Guidelines 1.4 • Assign custom policy OIDs for each Certificate type
3.9	Oct 2019	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

		<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 • Explicitly forbid MiTM Certificates • Clarify disclosure practice of end-entity certificates on the Repository

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** 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 (<http://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 319 411-1 v1.2.2. This audit is consistent with standards technical specification Electronic Signatures and Infrastructures (ESI); “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 v2.2.2. This audit is consistent with standards technical specification 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” under the scope QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QCP-w.
- ETSI EN 319 421 v1.1.1. This audit is consistent with standards technical specification Electronic Signatures and Infrastructures (ESI); “Policy and security requirements for Trust Service Providers issuing Time-Stamps” under the scope BTSP.
- Qualified Trust Service Provider (QTSP), following the Regulation (EU) N° 910/2014 (e-IDAS) of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

In addition to the above standards, HARICA complies with ETSI TS 119 495 v1.4.1 that supports Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366 and the Delegated Regulation (EU) 2018/389 with regard to Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication.

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 IETF RFC 3647. HARICA conforms to the current version of the

- “Baseline Requirements for the Issuance and Management of Publicly-Trusted 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” and
- “Guidelines for the Issuance and Management of Extended Validation Code Signing 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: 1.3.6.1.4.1.26513.1.0.4.2 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
4.2	First and Second digit of the version number of the Certification Practice Statement

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. The validity period of the HaricaRootCA2011 certificate is twenty (20) years (it shall be decommissioned by year 2030) and of the HaricaRootCA2015 and HaricaECCRootCA2015 is twenty-five (25) years. 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 RFC 5280 and according to policies set forth by the Root programs of Mozilla/Microsoft/Apple and comply with the EU Regulation 910/2014 (eIDAS). In the case of Externally Operated Subordinate CAs, an OID with the Subordinate CA’s CP/CPS MUST 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 and the corresponding Subordinate CA Certificate must be Technically Constrained to the Affiliate organization and Domain Namespace according to section 7.1.5.

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

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 this CP/CPS and Article 20 of Regulation (EU) 910/2014 (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 Regulation (EU) No 910/2014, 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. 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

Fax: +30-2310 999100

Ioannis Salmatzidis [jsal at it.auth.gr]

Tel: +30-2310 998498

Fax: +30-2310 999100

Spiros Bolis [sbol at gunet.gr]

Tel: +30-210 7275611

Fax: +30-210 7275601

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

Fax: +30-2310 999100

1.5.4 CPS approval procedures

The CP/CPS is approved by the Policy Management Committee. All amendments and updates since 13-5-2011 shall be posted at a publicly accessible Repository.

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

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

1.6 Definitions and acronyms

1.6.1 Definitions

Advanced Electronic Seal: An electronic signature that meets the requirements of Article 36 of Regulation (EU) 910/2014.

Advanced Electronic Signature: An electronic signature that meets the requirements of Article 26 of Regulation (EU) 910/2014.

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 issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: 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 Domain Name used to obtain authorization for certificate issuance for a given FQDN. HARICA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character (*), then HARICA MUST remove all wildcard labels from the left most portion of requested FQDN. HARICA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values 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 basic Constraints field has the cA attribute set to TRUE.

CAA: From [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".

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 or a certificate template file used by CA software.

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.

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

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 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 Authorization Document: Documentation provided by, or HARICA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

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 Name: The label 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.

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.

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 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.).

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.

High Risk Region of Concern (HRRC): A geographic location where the detected number of Code Signing Certificates associated with signed Suspect Code exceeds 5% of the total number of detected Code Signing Certificates originating or associated with the same geographic area. This information is provided in Appendix D of the “Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates” document.

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 label assigned to a device that uses the Internet Protocol for communication.

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

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

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

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.

Legal Entity: An [association](#), [corporation](#), [partnership](#), [proprietorship](#), [trust](#), government entity or other entity with [legal standing](#) 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.

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.

OCSF 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.

Parent Company: A company that Controls a Subsidiary Company.

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.

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.

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.

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.

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 Regulation (EU) No 910/2014

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 Regulation (EU) No 910/2014

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 specified in Regulation (EU) No 910/2014.

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 Regulation (EU) No 910/2014.

Qualified Electronic Signature/Seal Creation Device: Also known as QSCD. An electronic signature creation device that meets the requirements of Annex II of Regulation (EU) No 910/2014.

Qualified Electronic Time-stamp: An electronic Time-stamp that meets the requirements of Article 42 of Regulation (EU) No 910/2014.

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.

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 the IANA has marked as reserved:

- <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>
- <http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml>

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.

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 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, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

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.

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 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

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
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
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	Qualified Signature/Seal Creation Device
QSealC	Qualified electronic Seal Certificate
QTSP	Qualified Trust Service Provider
QWAC	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	ITU Telecommunication Standardization Sector
NCA ¹	National Competent Authority
OCSP	On-line Certificate Status Protocol
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
PSD ²	Payment Services Directive 2
PSP ²	Payment Service Provider

¹ See Directive (EU) 2015/2366

² See Commission Delegated Regulation (EU) 2018/389

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

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 the Digital Certificates of the Certification Authorities (type X.509v3), Digital Certificates that are issued according to this CP/CPS, the CRL, 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>.

Software vendors for SSL/TLS Certificates may use the following web sites for User Agent Verification:

Root CA	Status	URL
Harica Root CA 2011	Valid	https://haricarootca2011-valid.harica.gr
	Revoked	https://haricarootca2011-revoked.harica.gr
	Expired	https://haricarootca2011-expired.harica.gr
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

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.

3.1.1.1 Certificate name compliance with Baseline Requirements

HARICA does not issue certificates containing internal server names and/or reserved IP addresses.

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. In cases where the common name (CN) or any other element would produce an ambiguous or non-unique DN, 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 common name (OID: 2.5.4.3)	If present, for SSL/TLS certificates, this field MUST contain an FQDN or an IP Address that is one of the values contained in the Certificate's subjectAltName extension. For Client, S/MIME or Code Signing certificates, this field MUST contain a representation of the Subject's name. For Client Certificates, "common name" is used for user-friendly representation of the Subject's name to represent itself. This name does not need to be 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 full registered Organization Name. For QCP-w, QCP-w-psd2 and EV Certificates , the interpretation of this attribute is explained in section 9.2.1 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 QCP-w, QCP-w-psd2 and EV Certificates , the interpretation of this attribute is explained in section 9.2.6 of the EV Guidelines
OrganizationIdentifier (OID: 2.5.4.97)	A unique identifier for the Organization
businessCategory (OID: 2.5.4.15)	For QCP-w, QCP-w-psd2 and EV Certificates only . This field 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 8.5.2, 8.5.3, 8.5.4 or 8.5.5 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 QCP-w, QCP-w-psd2 and EV Certificates only . These fields MUST 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 9.2.5 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:

- "countryName"
- "givenName" and "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 the FQDN of the device certificate (FQDN DNS) or an IP Address in the "Subject Alternative Name – SAN" extension. The "Common Name" 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, Certificates shall include at least the following attributes in the Certificate subject DN:

- "organizationName"
- "countryName"
- "localityName" ή "stateOrProvinceName"

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

- "serialNumber"
- "businessCategory"
- "jurisdictionCountryName" and/or "jurisdictionStateOrProvinceName" and/or "jurisdictionLocalityName".

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

- "organizationIdentifier"

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

Certificates for SSL/TLS and eSeal under the QCP-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",
- "streetAddress", "postalCode", "localityName", "stateOrProvinceName", "countryName" according to section 9.2.7 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. A Subscriber Distinguished Name shall never be re-assigned to another entity by the same Issuing CA.

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.

For EV SSL/TLS Certificates, HARICA takes all verification steps reasonably necessary to satisfy the EV Verification Requirements set forth in the CA/Browser Forum EV SSL/TLS Guidelines.

For EV Code Signing Certificates, HARICA takes all verification steps reasonably necessary to satisfy the EV Code Signing Verification Requirements set forth in the CA/Browser Forum Baseline Requirements for Code Signing Certificates.

3.2.1 Method to prove possession of private key

The identity of the Applicant is authenticated 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 (QCP+), 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 6.2.1 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 in its capacity as a legal representative of a Legal Entity (under the QCP-1 or QCP-1-qscd policy), then the Applicant must provide the necessary documentation including the Legal Entity's complete name, legal status as well as relevant Country/State/City-level registration 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. For Code Signing and EV Code Signing Certificates, HARICA shall determine whether the entity is identified as requesting a Code Signing Certificate from a High Risk Region of Concern and flag it as "high risk".

Verification of organization identity in any request for an Extended Validation Certificate shall follow the EV verification procedures described in the CA/B Forum EV Guidelines. HARICA discloses the Incorporating or Registration Agencies used for validating Organization Identities at the HARICA repository as described in section 2.1.

3.2.2.1 Identity

If the Subject Identity Information 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 the CA or a third party who is acting as an agent for the CA; 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.

3.2.2.2 DBA/Tradenname/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 Subject Identity Information 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 tradenames;
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.

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

1. When the FQDN **does not contain "onion"** as the rightmost label, HARICA SHALL validate the FQDN using at least one of the methods listed below in this sub-section 3.2.2.4; and

When the FQDN **contains "onion"** as the rightmost label, HARICA SHALL validate the FQDN in accordance with

2. 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.

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*

Not used.

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

Confirming the Applicant's control over the FQDN 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 MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

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 Domain Name Registrar as representing the Domain Name Registrant for every FQDN 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, if 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.

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

3.2.2.4.3 *Phone Contact with Domain Contact*

Not used.

3.2.2.4.4 *Constructed Email to Domain Contact*

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 labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 *Domain Authorization Document*

Not used.

3.2.2.4.6 *Agreed-Upon Change to Website*

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Request Token or Random Value contained:

1. in the content of a file; or
2. on a web page in the form of a "meta tag" (as defined in HTML)

This file or web page MUST be accessible under the `"/.well-known/pki-validation"` directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port.

1. The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value MUST 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 timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1).

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

HARICA SHALL NOT perform validation using this method after 2020-06-03. HARICA MAY continue to re-use information and validations for domains validated under this method per the applicable certificate data reuse periods.

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 label that begins with an underscore character.

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

- (i) thirty (30) days or
- (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1).

Note: Once the FQDN has been validated using this method, HARICA MAY also issue Certificates for other FQDNs that end with all the 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.

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.

3.2.2.4.9 Test Certificate

Not used.

3.2.2.4.10 *TLS Using a Random Number*

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.11 *Any Other Method*

This method has been retired and MUST 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.

Note: Once the FQDN has been validated using this method, HARICA MAY also issue Certificates for other FQDNs that end with all the 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 MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST 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 labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

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 MUST 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 labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.15 *Phone Contact with Domain Contact*

Confirm the Applicant's control over the FQDN by calling the Domain 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 Domain Contact phone number is listed for each Authorization Domain Name being verified and they provide a confirming response for each Authorization Domain Name.

In the event that someone other than a Domain Contact is reached, HARICA MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, HARICA may leave the Random Value and the Authorization Domain Name(s) being validated. The Random Value MUST 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.

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

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 MAY 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 MUST 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.

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

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 MUST be found using the search algorithm defined in RFC 8659 Section 3.

HARICA MUST 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 MUST 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.

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

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 MUST NOT appear in the request used to retrieve the file, and
2. HARICA MUST 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 Number:

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

HARICA follows redirects and the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code).
2. Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
3. Redirects MUST be to resource URLs with either via the "http" or "https" scheme.
4. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. HARICA MUST provide a Random Value unique to the certificate request.
2. The Random Value MUST remain valid for use in a confirming response for no more than 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 labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.19 *Agreed-Upon Change to Website - ACME*

Reserved.

3.2.2.4.20 *TLS Using ALPN*

Reserved.

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.

After July 31, 2019, 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 MUST 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 timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of this CP/CPS).

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 MUST 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 reuse 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.

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.

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 MUST 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 **MUST** 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.

3.2.2.5.6 ACME “http-01” method for IP Addresses

Reserved.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

Reserved.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, HARICA follows a documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (e.g. “*.com”, “*.co.uk”). This is done by regularly retrieving and consulting a “public suffix list” such as <http://publicsuffix.org/> (PSL).

If a wildcard would fall within the label immediately to the left of a registry-controlled or 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 except as permitted under Appendix F of the EV Guidelines.

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.

Effective as of 1 October 2020, 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

HARICA must check for DNS CAA records for each `dNSName` in the `subjectAltName` extension of the certificate to be issued, according to the procedure in RFC 8659. If HARICA decides to issue a certificate that includes a `dNSName`, it MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

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

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
- if an Affiliate of HARICA is the DNS Operator (as defined in [RFC 7719](#)) of the domain's DNS.

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 take reasonable measures 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 performs this check by

- a) requesting the Applicant to enter the email address at the initial certificate request form and a verification email is sent back with a Random Value. Once the Applicant returns this Random Value back to HARICA, the email address is validated; or
- b) requesting the Applicant to perform a validation for the domain portion of an email address as an Authorization Domain Name, using any of the allowed domain validation methods described in section 3.2.2.4.

HARICA SHALL NOT delegate validation of the domain portion of an email address to third parties.

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 performed for 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 MUST 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 Regulation (EU) 2014/910.

"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".

Specifically for the issuance of Qualified Certificates according to Regulation (EU) 2014/910, identity of natural or legal persons is verified according to Article 24

paragraph 1. HARICA is currently using identity verification methods (a) and (c) from this paragraph.

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 a username/password provided during initial registration.

The Applicant submits the application for a device certificate on a secure web interface and authenticates by presenting either a personal certificate or a username/password pair therefore proving his/her identity.

HARICA central RA 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's Central RA implements a procedure to determine the authorized individuals that can request certificates on behalf of an organization. Each organization may limit authorized certificate requestors.

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 Extended Validation Certificate requests (either EV SSL/TLS or EV Code Signing), HARICA shall follow procedures described in section 11.8 of the EV Guidelines to verify the authority of the request.

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.

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

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. In the special case of Qualified Certificates, a certificate can be revoked:

- after request from governmental regulatory authorities
- if during auditing procedures it is found to contain false or inaccurate information
- if there is a relevant court order and

- in case of violating local and European legislation.

3.4.2 Revocation request from Subscriber

The Subscriber can request a certificate revocation to a secure HARICA web 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 **MUST** 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 marks all previously revoked and/or rejected certificate requests and may use this information to identify subsequent suspicious certificate requests.

HARICA shall only issue QCP-w, QCP-w-psd2, EV SSL and EV Code Signing Certificates to Applicants which submit a complete Certificate Request and meet the requirements specified in sections 8.5 and 10.2 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 MUST 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.

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, provided that HARICA obtained the data or document from a source specified under Section 3.2 no more eight hundred and twenty five (825) days prior to issuing the Certificate.

For EV Certificates, except for reissuance of an EV Certificate under Section 11.14.2 of the EV Guidelines and except when permitted otherwise in Section 11.14.1 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 – thirteen (13) months;
- (B) Assumed name – thirteen (13) months;
- (C) Address of Place of Business – thirteen (13) months;
- (D) Verified Method of Communication – thirteen (13) months;
- (E) Operational existence – thirteen (13) months;
- (F) Domain Name – thirteen (13) months;
- (G) Name, Title, Agency, and Authority – thirteen (13) months, 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 thirteen-month 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 11.9 and 11.10 of the EV Guidelines.

HARICA MUST repeat the verification process for any information obtained outside the time limits specified above except when permitted otherwise under section 11.14.1 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 digital certificate is also checked. In case the Applicant is not eligible for a digital certificate or the application contains errors, the application is rejected.

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 these criteria, and is not 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.

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 6.2.1.

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.

Subscribers who wish to authorize HARICA to issue 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 already have CAA entries in their respective DNS zone and need a Certificate from HARICA MUST add a CAA record property “issue” or “issuewild”, including 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 Subordinate CA Certificates via its official repository and through repositories provided by Application Software Suppliers.

For SSL/TLS Certificates that need to be trusted by Application Software Suppliers, HARICA shall log these certificates 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

Applicants MUST accept (retrieve and install through a secure webpage) their new certificate within **thirty (30) days**, otherwise the certificate is revoked and the Applicant must repeat the application process. Applicants SHOULD confirm that they have checked all certificate elements and that they are correct, to retrieve their certificate. Finally, they MUST accept the terms of use as they are described in this CP/CPS and then receive the certificate, thus becoming Subscribers.

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 web page, 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 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 web page 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 certificate 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

Modification of certificate information is not permitted.

4.8.3 Processing certificate modification requests

Modification of certificate information is not permitted.

4.8.4 Notification of new certificate issuance to Subscriber

Modification of certificate information is not permitted.

4.8.5 Conduct constituting acceptance of the certificate

Modification of certificate information is not permitted.

4.8.6 Publication of the modified certificate by the CA

Modification of certificate information is not permitted.

4.8.7 Notification of certificate issuance by the CA to other entities

Modification of certificate information is not permitted.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

A certificate must be revoked when the fields it contains have changed or when the corresponding private key has been exposed or lost or when there is suspicion that it has been exposed or lost. In the latter case, 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.

Moreover, the certificate must 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.

HARICA SHALL revoke any Subscriber Certificate within twenty four (24) hours if one or more of the following occurs:

1. The Subscriber requests in writing that HARICA revoke the Certificate;

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;
3. HARICA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. HARICA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

HARICA SHOULD revoke a TLS certificate within twenty-four (24) hours and MUST revoke a Certificate within five (5) days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. HARICA obtains evidence that the Certificate was misused;
3. HARICA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. HARICA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name 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 the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name. 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;
5. [Reserved];
6. HARICA is made aware of a material change in the information contained in the Certificate;
7. HARICA is made aware that the Certificate was not issued in accordance with HARICA's Certificate Policy or Certification Practice Statement;
8. HARICA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. HARICA's right to issue Certificates under this CP/CPS expires or is revoked or terminated, unless HARICA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by HARICA's Certificate Policy and/or Certification Practice Statement; or
11. HARICA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

HARICA MUST revoke S/MIME certificates upon the occurrence of any of the following events:

1. HARICA obtains reasonable evidence that the certificate has been used for a purpose outside of that indicated in the certificate or in HARICA's subscriber agreement or terms of use;
2. HARICA receives notice or otherwise becomes aware that a subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use;
3. HARICA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted;
4. HARICA receives notice or otherwise becomes aware of a material change in the information contained in the certificate;
5. a determination that the certificate was not issued in accordance with HARICA's CP/CPS;
6. HARICA determines that any of the information appearing in the certificate is not accurate;

For Code Signing Certificates, Subscribers are expected to not intentionally include Suspect Code in their signed software. Intentionally signing Suspect Code is a violation of this CP/CPS. If a third party provides information that the certificate is compromised or has been used to sign Suspect Code, HARICA shall investigate the request and revoke the Code Signing Certificate.

In addition to the reasons mentioned above, HARICA shall revoke a **Qualified Certificate/Seal** if any of the following event occurs:

1. The National Supervisory Body, during its surveillance duties, conclude that a Qualified Certificate/Seal contains false or inaccurate information, not-conformant to the eIDAS Regulation or
2. HARICA declares termination of services with no successor solution or
3. HARICA becomes aware that the Subscriber no longer has the signing right, is declared non-existent, is deceased, taking into account that Qualified Certificates for electronic signatures are in all cases non-transferable or
4. HARICA receives a court order with a final judgement that orders HARICA to revoke a Qualified Certificate/Seal or
5. HARICA obtains evidence that the Private Key corresponding to a Qualified Certificate/Seal have been compromised and used by a third-party that is unrelated to the Subscriber

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

1. the authorization of the PSP has been revoked;
2. any PSP role included in the certificate has been revoked.

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 to **cert-problem-report AT harica.gr** 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 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.

In such a case, within two (2) business days of receipt of the request, HARICA MUST either revoke the certificate or inform the Application Software Supplier that it is conducting an investigation. If HARICA decides to conduct an investigation, it MUST 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 MUST 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 Certificates used for "Signing" revocation dates

When revoking a Certificate used for Code Signing, e-Signatures or e-Seals, HARICA shall work with the Subscriber to estimate a date and time ("reasonable date") of when the revocation should occur in order to mitigate the impact of revocation on validly signed objects (Code, Documents, Data). For key compromise events, this date should be the earliest date of suspected compromise. This "reasonable date" and time 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 MUST 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. A Certificate Revocation List shall include the status of a certificate at least until its expiration. Alternately, 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

The CRL SHALL be signed by the Issuing CA or an entity designated by HARICA.

The CRL must be updated and published:

- for end-entity Certificates, every **seven (7) days** at the latest. The CRL will be in effect for a maximum time of **seven (7) days**. In case of revocation of an end-entity Certificate, a new CRL shall be issued and published within **twenty-four (24) hours** from the revocation timestamp.
- for Subordinate CA certificates and end-entity Certificates that contain an EKU which includes id-kp-timeStamping (as defined in RFC 5280), at least every **twelve (12) months**. The CRL will be in effect for a maximum time of **twelve (12) months**.

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 **MUST** be published within **twenty-four (24) hours** from the revocation timestamp.

CRLs shall be stored in a protected environment to ensure their integrity and authenticity.

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)

HARICA operates a publicly available Online Certificate Status Protocol (OCSP) service that conforms with RFC 6960. The URL of this service is included in the issued certificates. The operation of an OCSP service is mandatory only for Certification Authorities that issue publicly trusted certificates. OCSP responses **MUST** 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 **MUST** 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.

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.

For the status of Subscriber Certificates:

- OCSP responses **MUST** have a validity interval greater than or equal to **eight (8) hours**;
- OCSP responses **MUST** have a validity interval less than or equal to **ten (10) days**;
- For OCSP responses with validity intervals less than sixteen (16) hours, HARICA **SHALL** update the information provided via an Online Certificate Status Protocol 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** update the information provided via an Online Certificate Status Protocol at least **eight (8) hours** prior to the `nextUpdate`, and no later than **four (4) days** after the `thisUpdate`.

For the status of Subordinate CA Certificates:

- HARICA **SHALL** update information provided via an Online Certificate Status Protocol 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 "unused", 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 **MUST NOT** respond with a "good" status for such requests.

The OCSP responder **MAY** provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met.

4.9.11 Other forms of revocation advertisements available

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

If a Subscriber Certificate used for SSL/TLS is for a high-traffic FQDN, HARICA may rely on stapling, in accordance with RFC 6066, to distribute its OCSP responses. In this case, HARICA shall ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. HARICA shall enforce this requirement on the Subscriber either contractually, through the Subscriber Agreement or Terms of Use, or by technical review measures. HARICA may also issue such a Certificate with the "id-pe-tlsfeature" extension, per RFC 7633 including the "status_request" value as described in RFC 6066.

4.9.12 Special requirements re-key compromise

As defined in section 4.9.1.

4.9.13 Circumstances for suspension

Certificate suspension is permitted only for Certificates used for “Signing” (Code Signing, e-signature, e-seal, S/MIME). 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 only for “Signing Certificates” 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 used for “Signing” 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 used for “Signing”, 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.

HARICA SHALL provide OCSP Responses for Certificates used for e-Signatures, e-Seals, Code Signing and Timestamp for at least **seven (7)** years beyond expiry of such a Certificate. Application Software Suppliers MAY request HARICA to support a longer life-time according to their trust store requirements.

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 within any end-entity Certificate in CRL Distribution Points (where applicable) 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

HARICA's online certificate repository offers a web-based certificate search engine, supporting queries that contain the serial number or a part of the Distinguished Name of the certificate. The search results include the certificate's information and an indication on whether the certificate is valid or if it has been revoked. The Certificate Repository must display all certificates issued / revoked. This certificate repository is available at <https://repo.harica.gr>.

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 uninterrupted - as possible - availability of its OCSP service.

4.10.3 Optional features

No stipulation.

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 key escrow services.

4.12.2 Session key encapsulation and recovery policy and practices

HARICA does not currently support key escrow services.

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 located in locked cabinets in locked server rooms. Access to the server rooms are monitored and controlled at all times.

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.

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 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 11.13 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 Public Key Infrastructure issues. 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.

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 policy / procedures documents and this CP/CPS.

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 arranged and the proper information is disseminated to the staff.

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. 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 5.4.3 and 5.4.1 respectively, including the archival requirements of section 5.5.2.

5.3.8 Documentation supplied to the personnel

Relevant documentation is available from GUnet and offered 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 details of the 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 and OCSP entries;
 6. 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; and
 5. Generation of Certificate Revocation Lists and OCSP entries.
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. Firewall and router activities; and
 7. Entries to and exits from the CA facility.

Log records SHALL include the following elements:

1. Date and time of record;

2. Identity of the person making the journal record; and
3. Description of the record.

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

5.4.2 Frequency of processing log

All transactions are archived daily.

5.4.3 Retention period for audit log

HARICA 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 revocation or 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, supervised by the security administrator.

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.

5.5.2 Retention period for archive

HARICA shall retain records relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least

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

after the expiration date of the Certificate. Time-Stamping Certificates are valid for ten (10) years but require re-keying every year. So, logs for Time-Stamping Certificates are retained for eleven (11) years.

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

The 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.

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 incidents relating to Qualified Certificates for electronic signatures/seals, all provisions of article 19 of Regulation (EU) No. 910/2014 apply for the notification of the National supervisory body.

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 MUST 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.

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, 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 accredited 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.

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 **MUST** comply with the hardware standards defined in section 6.2.1. TSU Key Pairs are also generated in a secure environment by personnel in trusted roles under, at least, dual control.

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.

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 presence of an authorized person of the Registration Authority to attest that the key generation takes place in a crypto-token hardware device as defined in section 6.2.1; or
- receive a crypto-token hardware device as defined in section 6.2.1 that contains pre-generated Keys generated by authorized HARICA staff members operating in a Trusted Role capacity, following the process described in section 6.1.2; 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 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. HARICA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
5. HARICA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see <https://wiki.debian.org/SSLkeys>).

HARICA shall also reject a certificate request if it contains a Public Key previously used in a certificate that is revoked due to the corresponding Private Key being compromised.

6.1.2 Private Key delivery to Subscriber

The creation of private keys by any entity on behalf of an Applicant or another entity or from HARICA or a subCA on behalf of the Subscriber is generally not allowed. Key Pair generation on behalf of a Subscriber is not allowed for Keys that are to be associated with Certificates used for SSL/TLS.

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 certificate that include the Public Key corresponding to the communicated Private Key.

Private Keys may be 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.

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. ROOT 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](#)). 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 ECDSA key pairs, HARICA SHALL:

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

CAs that issue certificates with the codeSigning extended key usage set, MUST chain up to a CA with a minimum of RSA 4096-bit modulus or ECC NIST-P384 and MUST 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 the Subscribers, but 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.

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

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 (i.e. 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

All CA and TSU private keys MUST be stored in a secure Hardware Security Module to perform key signing operations, which MUST comply with at least FIPS PUB 140-2 level 3 or equivalent EAL 4+ or higher in accordance to ISO/IEC 15408 specifications. Special controls are in place to ensure that the hardware has not been tampered and is functioning correctly. CA and TSU private keys cannot be extracted in any form and are not accessible outside the Hardware Security Module.

Subscriber private keys can be generated and stored either in software or hardware cryptographic modules.

For Code Signing Certificates, HARICA MUST obtain a representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate private keys:

1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber’s private key protection through a TPM key attestation.

2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

For EV Code Signing Certificates, HARICA MUST ensure that the Subscriber's Private Key is generated, stored and used in a crypto module that meets or exceeds the requirements of:

- FIPS 140-2 level 2; or
- Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all parts applicable to the device type) or standards such as CEN EN 419 241 series or equivalent, for remotely managed devices; or
- by an EU Member State as a Qualified Signature Creation Device (QSCD) after 1 July 2016, or that was recognized as a Secure Signature Creation Device (SSCD) by an EU Member State designated body before 1 July 2016.

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 MUST be generated and stored in a QSCD and cannot be extracted in any form. QSCD devices MUST 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 Regulation (EU) 2014/910:

- <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.

6.2.2 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 **MUST** 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.

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.

6.2.7 Private Key storage on cryptographic module

All CA and TSU private keys **MUST** be stored in a secure Hardware Security Module to perform key signing operations. Subscriber private keys can also be generated on a hardware cryptographic module. In the special case of Qualified Certificates for Qualified electronic signatures/seals, the private key **MUST** be generated in a SSCD or a QSCD and cannot be extracted in any form.

Cryptographic modules for certain types of certificates **MUST** meet certain specifications, described in section 6.2.1.

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, OCSP Certificate signing 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.

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 is defined as:

- **twenty-five (25) years** for Root CA Certificates,
- **fifteen (15) years** for Subordinate CA Certificates,
- **three (3) years** for Client Authentication, Document Signing and S/MIME Certificates,
- **two (2) years** for SSL/TLS and Code Signing 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 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 is defined as:

- **twenty-five (25) years** for a Root CA Certificate,
- **fifteen (15) years** for a Subordinate CA Certificate,
- **three (3) years** for Client Authentication, Document Signing and S/MIME Certificates,
- **two (2) years** for Code Signing Certificates,
- **three hundred ninety seven (397) days** for SSL/TLS Certificates,
- **ten (10) years** for a Time-Stamping Unit or EV Timestamp Certificate.

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

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.

6.6.3 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.

6.8 *Time-stamping*

HARICA operates as a Qualified Time-Stamping Authority.

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 shall 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.

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.

Technically constrained Subordinate CA Certificates use the Name Constraints extension, described in Section 7.1.5 which is marked as “non-critical”. This is an exception to RFC 5280 (4.2.1.10) which is allowed by the CA/Browser Forum Baseline Requirements, until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

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.

- `basicConstraints` (critical): Indicates if the subject of the Digital Certificate is a CA and the maximum depth of valid certification paths that include this certificate. Uses value `CA=true` for CAs. It is omitted for end-entity certificates
- `keyUsage` (critical): Defines the purpose of the key contained in the Certificate. For CAs, it takes values `digitalSignature`, `keyCertSign` and `cRLSign`. For end-entity certificates, possible values include `digitalSignature` (authentication),

nonrepudiation (signing but only used with *digitalSignature* bit), *keyEncipherment* (encryption).

- *certificatePolicies*: explained in section 7.1.6
- *cRLDistributionPoints* (not critical): Identifies a URL for the Certificate Revocation List of the certificate's Issuing CA
- *authorityInformationAccess*: Indicates OCSP responder's URL and may also include the URL for the issuing CA's certificate.
 - For CA Certificates, it MAY contain the HTTP URL of the Issuing CA's OCSP responder (*accessMethod* = 1.3.6.1.5.5.7.48.1).
 - For End-Entity Certificates it MUST contain the HTTP URL of the Issuing CA's OCSP responder (*accessMethod* = 1.3.6.1.5.5.7.48.1).
- Authority Key Identifier: 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
- Subject Key Identifier: Identifies a particular Public Key uniquely. It contains the ID of the Certificate Holder's key
- Subject Information: As specified in section 7.1.4.7
- Subject Alternative Name (required for SSL/TLS and S/MIME Certificates): It provides multiple values for email address, Microsoft UPN, a DNS name or a Uniform Resource Identifier (URI)
- Extended Key Usage (EKU): Indicates one or more purposes for which the certificate may be used. It may contain the following values
 - *serverAuth* (OID: 1.3.6.1.5.5.7.3.1)
 - *clientAuth* (OID: 1.3.6.1.5.5.7.3.2)
 - *codeSigning* (OID: 1.3.6.1.5.5.7.3.3)
 - *emailProtection* (OID: 1.3.6.1.5.5.7.3.4)
 - IP Sec EndSystem (OID: 1.3.6.1.5.5.7.3.5)
 - IP Sec Tunnel (OID: 1.3.6.1.5.5.7.3.6)
 - IP Sec User (OID: 1.3.6.1.5.5.7.3.7)
 - *TimeStamping* (OID: 1.3.6.1.5.5.7.3.8)
 - *OCSP Signing* (OID: 1.3.6.1.5.5.7.3.9)
 - *smartcardlogon* (OID: 1.3.6.1.4.1.311.20.2.2)
 - *Encrypting File System* (OID: 1.3.6.1.4.1.311.10.3.4)
 - *Document Signing* (OID: 1.3.6.1.4.1.311.10.3.12)
 - *Lifetime Signing* (OID: 1.3.6.1.4.1.311.10.3.13)

A single Issuing CA MUST NOT be used to issue certificates that blend the *id-kp-serverAuth* [RFC5280], the *id-kp-emailProtection* [RFC5280], the *id-kp-codeSigning* [RFC5280] and the *id-kp-timeStamping* [RFC5280] values in the EKU extension. After this effective date, new Issuing CAs must separate Server Authentication, S/MIME, Code Signing and Time Stamping Extended Key Usages. **Effective June 1 2020**, the *id-kp-ocspSigning* [RFC5280] value MUST NOT be used in a CA Certificate's EKU extension.

- Qualified Certificate Statements (*qcStatements*): If the Certificate is used in compliance with Regulation (EU) No. 910/2014, 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 Regulation (EU) No. 910/2014 and MUST always be present in Certificates for Advanced/Qualified electronic signatures/seals. Additionally, Certificates for Qualified electronic signatures/seals MUST include the value “id-etsi-qcs-QcSSCD”, which asserts that the private key was generated in an SSCD/QSCD. Additional values are allowed and MUST follow the requirements described in ETSI EN 319 412-1.

- PSD2 Qualified Certificate Statements: If the Certificate is used in compliance with Regulation (EU) No. 2018/389 and Directive (EU) 2015/2366, this extension contains special attributes/values to convey information about Payment Service Providers to Relying Parties.
 - the role of the payment service provider, which maybe 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.
- CA/Browser Form Organization Identifier: If the `subject:organizationIdentifier` field is present, this field MUST be present in a special CA/Browser Forum extension. This extension shall follow the requirements of sections 9.2.8 and 9.8.2 of the EV Guidelines.

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 MUST 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 TLS/SSL 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 MUST be present, and MUST 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 MUST 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 MUST use the `namedCurve` encoding.

- For P-256 keys, the `namedCurve` MUST be `secp256r1` (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the `namedCurve` MUST be `secp384r1` (OID: 1.3.132.0.34).
- For P-521 keys, the `namedCurve` MUST be `secp521r1` (OID: 1.3.132.0.35).

When encoded, the `AlgorithmIdentifier` for ECDSA keys MUST 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`.

7.1.3.2 Signature AlgorithmIdentifier

For SSL/TLS Certificates, all objects signed by a CA Private Key MUST conform on the use of the `AlgorithmIdentifier` or `AlgorithmIdentifier-derived` type in the context of signatures. In particular, 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` MUST 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:
`304106092a864886f70d01010a3034a00f300d0609608648016503040201`
`0500a11c301a06092a864886f70d010108300d0609608648016503040201`
`0500a203020120`
- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:
Encoding:
`304106092a864886f70d01010a3034a00f300d0609608648016503040202`
`0500a11c301a06092a864886f70d010108300d0609608648016503040202`
`0500a203020130`
- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

Encoding:

304106092a864886f70d01010a3034a00f300d0609608648016503040203
0500a11c301a06092a864886f70d010108300d0609608648016503040203
0500a203020140

In addition, HARICA MAY use the following signature algorithm and encoding if all of 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: 2.5.2937.0) 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 MUST 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) `keyPurposeIdr`.
- 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 the following 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 MUST use ECDSA with SHA-256. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040302.

- If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040303`.
- If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040304`.

7.1.4 Name Forms

7.1.4.1 Serial number

Unique system generated number assigned to each certificate. No duplicate serial numbers are 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-1 and QCP-1-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: "NTRGR-123456789". In this example, GR is the Subject's Country.
 - Legal Entity's Tax Identification Number with the following semantics: "VATGR-123456789".
- `organizationName` (OID: 2.5.4.10) (Required): This field MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2. 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 MUST 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 MUST contain an FQDN or an IP Address that is one of the values contained in the Certificate's subjectAltName extension. For Client, S/MIME or Code Signing certificates, this field MUST contain a representation of the Subject's name as verified under section 3.2.2.1. Common names that also belong to the DNS namespace are forbidden for non-SSL certificates.
- givenName (OID: 2.5.4.42) and 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.
- **organizationName** (OID: 2.5.4.10): Subject Organization Name as verified under section 3.2.2.1. For EV Certificates, this attribute must be verified according to section 9.2.1 of the EV Guidelines.
- **localityName** (OID: 2.5.4.7) (Optional if “State or Province” is present): Subject Locality as verified under section 3.2.2.1
- **stateOrProvinceName** (OID: 2.5.4.8) (Optional if “Locality” is present): Subject State as verified under section 3.2.2.1
- **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 **MUST** chain up to a 4096-bit RSA or ECC equivalent (P384) CA.
- **serialNumber** (OID: 2.5.4.5) (Required for EV, QCP-w)(Optional for LCP, NCP, NCP+, QCP-n, QCP-n-qscd):
 - Per EV and QCP-w it contains the Registration Number of the Legal Entity of the Subject.
 - For Private Organizations, this field **MUST** 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:
 - Social Security Number with the following semantics: "PNOGR-12345678". In this example, GR is the Subject's Country.
 - Personal Identification Card with the following semantics: "IDCGR-AK1234567". In this example, GR is the Subject's Country.
 - Tax Identification Number with the following semantics: "TINGR-123456789".
 - Passport Number with the following semantics: "PASGR-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 8.5.2, 8.5.3, 8.5.4 or 8.5.5 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 9.2.5 of the EV Guidelines.
- OrganizationIdentifier (OID: 2.5.4.97): Per QCP-1 and QCP-1-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: "NTRGR-123456789". In this example, GR is the Subject's Country.
 - Legal Entity's Tax Identification Number with the following semantics: "VATGR-123456789".For PSD2 Certificates, the semantics shall follow clause 5.1.4 of ETSI TS 119 412-1 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.
- With the exception of EV Certificates, other subjectDN attributes MAY be present within the subject field. If present, other attributes MUST 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 MUST 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.

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.

7.1.4.8 Subject Alternative Name Extension

This extension is Required for SSL and S/MIME Certificates and is Optional for Code Signing Certificates.

Contents for SSL/TLS Certificates: This extension must contain at least one entry. Each entry must be a dNSName type containing the Fully-Qualified Domain or an iPAddress type containing a validated IP address. HARICA must confirm that the Applicant controls the Fully-Qualified Domain Name or has been granted the right to use it by the Domain Name Registrant per section 3.2.2.4. For an IP address, HARICA must confirm that the Applicant controls the IP Address or has been granted the right to use it per section 3.2.2.5. Wildcard Domain Names are permitted. Certificates containing underscore characters ("_") in domain labels in dNSName entries MUST NOT be present. Wildcard Certificates are not allowed for EV SSL/TLS Certificates except as permitted under Appendix F of the EV Guidelines. Wildcard Domain Names are allowed for DV and OV SSL/TLS Certificates, taking into account the provisions of section 3.2.2.6.

Contents for Code Signing Certificates: If this field is present, it shall not contain dNSName, iPAddress or other entries that point to a Domain Name or IP Address.

Contents for S/MIME Certificates: This extension must contain at least one entry. Each entry must be an rfc822Name containing an email address of the Subscriber. It

must not contain a Domain Name or IP Address. HARICA must confirm that the Applicant controls the email address per section 3.2.3.1.

7.1.5 Name constraints

HARICA uses the name constraints extension per RFC 5280, in order to limit the scope of Subordinate CAs. This extension is marked as “non-critical”.

Each Institution’s Subordinate CA Certificate MUST be constrained to one or more Domain Namespace owned by that Institution. For example, Aristotle University of Thessaloniki Subordinate CA Certificate is limited to the “auth.gr” Domain Namespace, using the name constraints extension.

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate MUST 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 MUST NOT appear within this extension.

If a Subordinate CA Certificate includes the id-kp-serverAuth extended key usage and the respective Subordinate CA needs to be treated as technically constrained and audited as described in section 8.7, then the Subordinate CA Certificate MUST include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

- a) For each dNSName in permittedSubtrees, HARICA MUST 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 MUST 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 MUST 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 extended key usage and the respective Subordinate CA needs to be treated as technically constrained and audited as described in section 8.7 and not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate MUST specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate MUST 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 MUST also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate MUST include at least one iPAddress in permittedSubtrees.

If the Subordinate CA Certificate includes an extended key usage other than the “id-kp-serverAuth” it is treated as technically constrained and audited as described in section 8.7.

Moreover, HARICA ROOT CA 2011 is limited to the following domains: .gr, .eu, .edu, .org.

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
- **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
- **QCP-w** (Qualified Website Authentication Certificate)
 - **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
- **QCP-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
 - 1.3.6.1.4.1.26513.1.1.2.3.1
 - 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
 - 1.3.6.1.4.1.26513.1.1.2.2.3
 - 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 POLICY IDENTIFIERS.

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.

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 MUST follow the requirements described in sections 6.1.5 and 6.1.6.

7.2.2.2 Hashing Algorithm

The hashing algorithm **MUST** 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.

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 **MUST 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 **MUST** be included and **MUST 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 **MUST** be included and **MUST 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 Expired certificates on CRL (OID: 2.5.29.60)

This extension **MAY** be present and **MUST 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 Reason Code (OID 2.5.29.21)

If present, this CRL entry extension **MUST NOT** be marked critical.

Effective 2020-09-30 and applicable only 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 **MUST** be present.

Effective 2020-09-30, 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 **MUST NOT** be unspecified (0). If the reason for revocation is unspecified, Issuing CAs **MUST** omit reasonCode entry extension, if allowed by the previous requirements. If a CRL entry is for a SSL/TLS Certificate, the CRLReason **MUST NOT** be certificateHold (6). See section 4.9.15 for more information.
- If a reasonCode CRL entry extension is present, the CRLReason **MUST** indicate the most appropriate reason for revocation of the certificate based on section 9.5.3.1 of the ITU-T X.509 recommendation and RFC 5280.

7.3 OCSP Profile

The Online Certificate Status Protocol (OCSP) is used to validate the revocation status of all certificates signed by the Root Certification Authority. The use of OCSP is mandatory for all Subordinate CAs.

The OCSP responders **MUST** conform to RFC 6960.

Effective 2020-09-30, 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 **MUST** be present.

Effective 2020-09-30, the CRLReason indicated **MUST** 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 **MUST 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

HARICA SHALL at all times issue Certificates and operate its PKI in accordance with all applicable law and the requirements of this CP/CPS.

8.1 Frequency or circumstances of assessment

CA Certificates that are capable of being used to issue new certificates MUST 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.

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 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 (e-IDAS) of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

HARICA has also included guidelines and procedures from the following documents:

- “Baseline Requirements for the Issuance and Management of Publicly-Trusted 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” and
- “Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates”,

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 under the payment services Directive (EU) 2015/2366 and the Delegated Regulation (EU) 2018/389 with

regard to Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication.

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 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.

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 11.13 of the EV Guidelines is performed by an external RA, HARICA MUST 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.

If HARICA uses a third-party entity to participate in the validation process for the issuance of EV Certificates, HARICA SHALL contractually obligate each third-party Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in the 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.

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 to 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.

9.5 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, Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates, Mozilla and Microsoft Root Program Requirements are used in this CP/CPS.

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 MUST 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 MUST 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 and the Terms of Use.

The Subscriber or Terms of Use Agreement 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.
- ✓ Subscribers must create a key pair (private and public) using a reliable and secure system and take all necessary precautions to protect their private key 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.
- ✓ Especially in case of code signing, Subscribers are bound by the RA 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.
- ✓ **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times 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 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.
- ✓ they must use Time-Stamps from HARICA TSUs in combination with a valid signing (un-revoked) Certificate

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 statute 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.

In the event that 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 (with the exception of 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.

With the exception of 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 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.

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 MUST also (prior to issuing an SSL/TLS certificate under the modified requirement) 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 MUST 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, MUST 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 and every 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 of the particular obligation on the part of HARICA 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 2011 ====

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011

Validity

Not Before: Dec 6 13:49:52 2011 GMT

Not After : Dec 1 13:49:52 2031 GMT

Subject: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:a9:53:00:e3:2e:a6:f6:8e:fa:60:d8:2d:95:3e:
f8:2c:2a:54:4e:cd:b9:84:61:94:58:4f:8f:3d:8b:
e4:43:f3:75:89:8d:51:e4:c3:37:d2:8a:88:4d:79:
1e:b7:12:dd:43:78:4a:8a:92:e6:d7:48:d5:0f:a4:
3a:29:44:35:b8:07:f6:68:1d:55:cd:38:51:f0:8c:
24:31:85:af:83:c9:7d:e9:77:af:ed:1a:7b:9d:17:
f9:b3:9d:38:50:0f:a6:5a:79:91:80:af:37:ae:a6:
d3:31:fb:b5:26:09:9d:3c:5a:ef:51:c5:2b:df:96:
5d:eb:32:1e:02:da:70:49:ec:6e:0c:c8:9a:37:8d:
f7:f1:36:60:4b:26:2c:82:9e:d0:78:f3:0d:0f:63:
a4:51:30:e1:f9:2b:27:12:07:d8:ea:bd:18:62:98:
b0:59:37:7d:be:ee:f3:20:51:42:5a:83:ef:93:ba:
69:15:f1:62:9d:9f:99:39:82:a1:b7:74:2e:8b:d4:
c5:0b:7b:2f:f0:c8:0a:da:3d:79:0a:9a:93:1c:a5:
28:72:73:91:43:9a:a7:d1:4d:85:84:b9:a9:74:8f:
14:40:c7:dc:de:ac:41:64:6c:b4:19:9b:02:63:6d:
24:64:8f:44:b2:25:ea:ce:5d:74:0c:63:32:5c:8d:
87:e5

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

X509v3 Key Usage:

Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:

A6:91:42:FD:13:61:4A:23:9E:08:A4:29:E5:D8:13:04:23:EE:41:25

X509v3 Name Constraints:

Permitted:

DNS:.gr

DNS:.eu

DNS:.edu

DNS:.org

email:.gr

email:.eu

email:.edu

email:.org

Signature Algorithm: sha1WithRSAEncryption

1f:ef:79:41:e1:7b:6e:3f:b2:8c:86:37:42:4a:4e:1c:37:1e:
8d:66:ba:24:81:e9:4f:12:0f:21:c0:03:97:86:25:6d:5d:d3:
22:29:a8:6c:a2:0d:a9:eb:3d:06:5b:99:3a:c7:cc:c3:9a:34:
7f:ab:0e:c8:4e:1c:e1:fa:e4:dc:cd:0d:be:bf:24:fe:6c:e7:
6b:c2:0d:c8:06:9e:4e:8d:61:28:a6:6a:fd:e5:f6:62:ea:18:
3c:4e:a0:53:9d:b2:3a:9c:eb:a5:9c:91:16:b6:4d:82:e0:0c:
05:48:a9:6c:f5:cc:f8:cb:9d:49:b4:f0:02:a5:fd:70:03:ed:
8a:21:a5:ae:13:86:49:c3:33:73:be:87:3b:74:8b:17:45:26:
4c:16:91:83:fe:67:7d:cd:4d:63:67:fa:f3:03:12:96:78:06:
8d:b1:67:ed:8e:3f:be:9f:4f:02:f5:b3:09:2f:f3:4c:87:df:
2a:cb:95:7c:01:cc:ac:36:7a:bf:a2:73:7a:f7:8f:c1:b5:9a:
a1:14:b2:8f:33:9f:0d:ef:22:dc:66:7b:84:bd:45:17:06:3d:
3c:ca:b9:77:34:8f:ca:ea:cf:3f:31:3e:e3:88:e3:80:49:25:
c8:97:b5:9d:9a:99:4d:b0:3c:f8:4a:00:9b:64:dd:9f:39:4b:
d1:27:d7:b8

=== END HARICA ROOT CA 2011 ===

=== 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:

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

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:

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

```
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:

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

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 ===

11 ANNEX B (HARICA Common Certificate Profiles)

Friendly Name	Policy IDs	Key Usages	Other Extensions
HARICA Internally Operated Subordinate 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 Encipherment³ 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 Encipherment³ 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 Encipherment³ 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 Encipherment³ EKU: TLS Web Client Authentication, Email Protection, MS Document Signing	None

³ “Key Encipherment” is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

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 Encipherment³ EKU: TLS Web Client Authentication, Email Protection, MS Document Signing	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: Digital Signature, Key Encipherment³ (allowed when combined with S/MIME) EKU: TLS Web Client Authentication, MS Document Signing, Email Protection (optional)	QcStatements: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-esign, id-etsi-qcs-SemanticsId-Natural(optional)

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

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, 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: Digital Signature, Key Encipherment³ (allowed when combined with S/MIME) EKU: TLS Web Client Authentication, MS Document Signing, 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, 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 Web Authentication	0.4.0.194112.1.4 (QCP-w), 2.23.140.1.1, 1.3.6.1.4.1.26513.1.1.1.5	KU: Digital Signature, Key Encipherment³ 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)

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

Qualified Certificate for PSD2 Web Authentication	0.4.0.19495.3.1 (QCP-w-psd2), 2.23.140.1.1, 1.3.6.1.4.1.26513.1.1.1.6	KU: Digital Signature, Key Encipherment³ 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
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	QcStatements: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS
IV Code Signing	0.4.0.2042.1.1 (NCP), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.2.1	KU: Digital Signature EKU: Code Signing, Lifetime Signing (optional)	None
OV Code Signing	0.4.0.2042.1.1 (NCP), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.1.1	KU: Digital Signature EKU: Code Signing, Lifetime Signing (optional)	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

Hellenic Academic and Research Institutions Certification Authority (HARICA)
Public Key Infrastructure
Certificate Policy and Certification Practice Statement (v4.1)

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 Encipherment³ 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 Encipherment³ 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 Encipherment³ 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 Encipherment³ 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.

12.1 Unconstrained Subordinate CAs

- Hellenic Academic and Research Institutions ECC RootCA 2015
 - HARICA EV TLS ECC SubCA R1
 - HARICA QWAC ECC SubCA R1
 - HARICA SSL ECC SubCA R2
- Hellenic Academic and Research Institutions RootCA 2011
 - HARICA SSL Intermediate CA R1
- Hellenic Academic and Research Institutions RootCA 2015
 - HARICA EV TLS RSA SubCA R1
 - HARICA QWAC RSA SubCA R1
 - HARICA SSL RSA SubCA R3

12.2 Technically Constrained Subordinate CAs

- Hellenic Academic and Research Institutions ECC RootCA 2015
 1. HARICA Administration Client ECC SubCA R2
 2. HARICA Administration SSL ECC SubCA R2
 3. HARICA Client Authentication ECC SubCA R2
 4. HARICA Code Signing ECC SubCA R2
 5. HARICA EV Code Signing ECC SubCA R1
 6. HARICA Qualified Legal Entities ECC SubCA R2
 7. HARICA Qualified Natural Entities ECC SubCA R2
 8. HARICA S/MIME ECC SubCA R2
- Hellenic Academic and Research Institutions RootCA 2011
 1. Academy of Athens Client CA R1
 2. Aristotle University of Thessaloniki Central CA R5
 3. Athens University of Economics and Business CA R2
 4. CEDEFOP CA R1
 5. Democritus University of Thrace CA R1
 6. Eastern Macedonia and Thrace Institute of Technology CA R1
 7. Greek Academic Network CA R2
 8. Greek School Network CA R2
 9. HARICA Client Authentication RSA SubCA R1
 10. HARICA Qualified Legal Entities SubCA R1
 11. HARICA Qualified Natural Entities SubCA R1
 12. HARICA S_MIME RSA SubCA R1
 13. Harokopio University CA R1
 14. HEAL-LINK Hellenic Academic Libraries Link CA R2
 15. Hellenic Academic and Research Institutions AdminCA R6
 16. Institute of Accelerating Systems and Applications Client CA R1

17. Institute of Accelerating Systems and Applications SSL CA R1
 18. International Hellenic University CA R1
 19. Ionian University Client CA R1
 20. Ionian University SSL CA R1
 21. National and Kapodistrian University of Athens CA R2
 22. Panteion University of Social and Political Sciences CA R1
 23. Piraeus University of Applied Sciences CA R1
 24. Technical University of Crete CA R1
 25. Technological Educational Institute of Epirus CA R3
 26. Technological Educational Institute of Western Greece CA R1
 27. Technological Educational Institution of Central Macedonia CA R3
 28. Technological Educational Institution of Thessaloniki CA R3
 29. Technological Educational Institution of Thessaly CA R2
 30. University of Crete CA R3
 31. University of Ioannina CA R2
 32. University of Macedonia CA R1
 33. University of Patras CA R1
 34. University of Piraeus CA R1
 35. University of the Peloponnese CA R2
 36. University of Western Macedonia CA R3
- Hellenic Academic and Research Institutions RootCA 2015
 1. Academy of Athens SSL SubCA R2
 2. ACER Client RSA SubCA R2
 3. Aristotle University of Thessaloniki Client RSA SubCA R2
 4. Aristotle University of Thessaloniki Client RSA SubCA R3
 5. Aristotle University of Thessaloniki SSL RSA SubCA R2
 6. Athens University of Economics and Business Client RSA SubCA R1
 7. Athens University of Economics and Business TLS RSA SubCA R1
 8. CEDEFOP Client RSA SubCA R1
 9. CEDEFOP TLS RSA SubCA R1
 10. Democritus University of Thrace Client RSA SubCA R1
 11. Democritus University of Thrace TLS RSA SubCA R1
 12. Ecclesiastical Academy of Vella SSL RSA SubCA R2
 13. Greek Federation of Judicial Officers Client RSA SubCA R3
 14. Greek Federation of Judicial Officers Client RSA SubCA R4
 15. Greek Federation of Judicial Officers Client SubCA R2
 16. Greek School Network TLS RSA SubCA R1
 17. Greek Universities Network TLS RSA SubCA R1
 18. GRnet Client RSA SubCA R2
 19. GRNET Client RSA SubCA R4
 20. GRnet SSL RSA SubCA R2
 21. GRNET TLS RSA SubCA R1
 22. HARICA Client Authentication RSA SubCA R2
 23. HARICA EV Code Signing RSA SubCA R1
 24. HARICA Institutional Client SubCA R1
 25. HARICA Qualified Legal Entities SubCA R2
 26. HARICA Qualified Legal Entities SubCA R3
 27. HARICA Qualified Natural Entities SubCA R2

28. HARICA Qualified Natural Entities SubCA R3
29. HARICA Qualified Time Stamping RSA SubCA R1
30. HARICA S_MIME RSA SubCA R2
31. HARICA S_MIME RSA SubCA R3
32. Harokopio University Client RSA SubCA R1
33. Harokopio University TLS RSA SubCA R1
34. HEAL-LINK Hellenic Academic Libraries Link TLS RSA SubCA R1
35. Hellenic Academic and Research Institutions AdminCA R5
36. Hellenic Academic and Research Institutions Code Signing CA R1
37. Hellenic Academic and Research Institutions Time Stamping CA R1
38. Inst. of Accelerating Systems and Applications TLS RSA SubCA R1
39. International Hellenic University Client RSA SubCA R1
40. International Hellenic University TLS RSA SubCA R1
41. Ionian University Client RSA SubCA R2
42. Ionian University TLS RSA SubCA R1
43. Ministry of Digital Governance (Hellenic Republic) SubCA R1
44. National and Kapodistrian University of Athens TLS RSA SubCA R1
45. National and Kapodistrian Univ. of Athens Client RSA SubCA R1
46. National Technical University of Athens TLS RSA SubCA R1
47. Panteion Univ. of Social and Political Sciences Client SubCA R1
48. Panteion Univ. of Social and Political Sciences TLS RSA SubCA R1
49. Technical University of Crete Client RSA SubCA R1
50. Technical University of Crete TLS RSA SubCA R1
51. University of Crete Client RSA SubCA R1
52. University of Crete TLS RSA SubCA R1
53. University of Ioannina Client RSA SubCA R1
54. University of Ioannina TLS RSA SubCA R1
55. University of Macedonia Client RSA SubCA R1
56. University of Macedonia TLS RSA SubCA R1
57. University of Patras Client RSA SubCA R1
58. University of Patras TLS RSA SubCA R1
59. University of Piraeus Client RSA SubCA R1
60. University of Piraeus TLS RSA SubCA R1
61. University of the Aegean Client RSA SubCA R1
62. University of the Aegean TLS RSA SubCA R1
63. University of the Peloponnese Client RSA SubCA R1
64. University of the Peloponnese TLS RSA SubCA R1
65. University of West Attica Client RSA SubCA R1
66. University of West Attica TLS RSA SubCA R1
67. University of Western Macedonia Client RSA SubCA R1
68. University of Western Macedonia TLS RSA SubCA R1

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 **MUST** 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 **MUST** be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used. Global Numbers **MUST** have a preceding + and a country code and **MAY** contain 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 **MUST** be placed on the "_validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record **MUST** 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 **MUST** be placed on the "_validation-contactphone" subdomain of the domain being validated. The entire RDATA value of this TXT record **MUST** 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 RFC 7686 ".onion" special-use Domain Names in a Certificate.

1. The Domain Name MUST contain at least two labels, where the right-most label is "onion", and the label immediately preceding the right-most "onion" 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 MUST 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 3.2.2.4.6 or 3.2.2.4.18.
 - b. by having the Applicant provide a Certificate Request signed using the .onion public 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 with at least 64-bits of entropy that is generated by the Applicant.

The signing nonce attributes have the following format:

```
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 }
```

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 FQDN where "onion" is in the right-most label of the 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**
<http://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
	0			Central Certificate Policy/Certification Practice Statement
		3		First digit of the version number of the Central Certificate Policy/Certification Practice Statement
			8	Second digit of the version number of the Central Certificate Policy/Certification Practice Statement
		1		Certificate Policy for specific certificate type
		1		Server Authentication
			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
			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
			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
			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
			5	Qualified Website Authentication (QCP-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
			6	Qualified Website Authentication for PSD2 (QCP-w-psd2) compatible with - ETSI TS 119 495 OID 0.4.0.19495.1.1 - Regulation (EU) 910/2014 - Directive (EU) 2015/2366
		2		Email Signing
			1	Simple Email Validation (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
		3	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
	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
		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
		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
		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

		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 - 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 - 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
		7	OCSP Responder Certificate
		8	Remote QSCD