Greek Universities Network (GUnet)

Hellenic Academic and Research Institutions

Public Key Infrastructure

Hellenic Academic and Research Institutions Certification Authority (HARICA)

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

Version 3.5 (May 18th 2017)

Table of Contents

Version control

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

		• Incorporate Microsoft Root Certificate Program –Technical Requirements 2.0 • Incorporate Mozilla Root CA program Policy 2.2 • Adapt to Presidential Decree 150/2001 • Changes to certificate profiles and Policy OIDs
3.1	Feb 2015	• Adding qualified certificate extensions (qcStatements)
3.2	June 2015	• Changes at the allowed values of the Subject and the subjAltName extension • Disclosure of reviewing CAA records • Incorporate CA/B Forum BR 1.2.5
3.3	March 2016	• New Root CAs • Compliance to Updated Microsoft Root Program Policy • Incorporate CA/B Forum BR 1.3.1 • Improve compatibility with RFC3647 • Improve compatibility with RFC5480 (keyUsage bits for ECDSA certificates)
3.4	April 2016	• Refine language regarding the term “CA”, “TSP” • Added scope for cross-signing
3.5	May 2017	• Refine language regarding the term “Subordinate CA” • Changes to comply with ETSI EN 319 411-1. EN 319 411-2, EN 319 421 • Separate TimeStamping certificates from SSL, S/MIME, CodeSigning

		• Compliance with "Minimum Requirements of the Issuance and Management of Publicly-Trusted Code Signing Certificates" published at https://aka.ms/csbr (Effective date Feb 1st 2017) • Incorporate CA/B Forum BRs 1.4.5 • Change validity duration of end-entity SSL/Personal Certificates • New Insurance Contract for professional liability, updated liability rules

1 Introduction

The Public Key Infrastructure (PKI) for the Hellenic Academic and Research Institutions is supported and operated by the Greek Universities Network GUnet (http://www.gunet.gr), a non-profit organization with members all the Universities and Technological Educational Institutions of Greece. 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. 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 Certification 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 has been accredited and certified for its Public Key Infrastructure with:

- ETSI EN 319 411-1 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 certificates; Part1: General requirements" under the scope NCP, NCP+, LCP, DVCP, OVCP.
- ETSI EN 319 411-2 v2.1.1. 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.
- 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^{o} 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.

1.2 Document Name and identification

This document is called «Certification 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 Certification 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) 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 RFC3647. This document also adopts guidelines and specs from the CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" http://www.cabforum.org and the "Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" published at https://aka.ms/csbr.

The globally unique Identification Number (OID) of this document is: 1.3.6.1.4.1.**26513.1.0.3.5** 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
3.5	First and Second digit of the version number of the Certification Practice Statement

1.3 PKI Participants

The entities that use digital certificates issued by HARICA, constitute the community governed by this Certification Policy and Certification Practice Statement.

1.3.1 Certification Authorities

Certification Authorities (CAs) (a.k.a. Trust Service Providers) 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 RFC6960. 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. HARICA Internally Operated Subordinate CAs, some of 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 Certification 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 also 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 RFC5280 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.

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 participating 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 certificate, Relying Parties must check that:

- √ The validity period of the certificate has begun and has not expired.
- √ 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.
- √ They abide by the terms and the conditions as described in the present CP/CPS.

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 money transactions (e.g. credit-card payments via e-shop) or 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.

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 University 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 [d.zacharopoulos at auth.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 University 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 998492

1.5.3 Policy enforcement persons

cp at harica.gr
Dimitris Zacharopoulos [d.zacharopoulos at auth.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 University 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 998492

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 the main website of HARICA.

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 once a year 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, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate 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 or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant:

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

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

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

Audit Period: In a period- of- time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement.

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 6844: "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

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

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in 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 Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

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.

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 the CA but is authorized by HARICA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

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 contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record

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 assigns).

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

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

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 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.

Internally Operated Subordinate CA: A Subordinate CA Operator, 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.

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

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Key Generation Script: A documented plan of procedures for the generation of the Key Pair to be associated with a CA Certificate**.**

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

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

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.

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

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

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

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.

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

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

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

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

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

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

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.

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 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 RFC5280.

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

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

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.

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.

1.6.2 Acronyms

Short Term	Explained Term
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
DN	Distinguished Name
DVCP	Domain Validation Certificates Policy
EKU	Extended Key Usage
EVCP	Extended Validation Certificates Policy
FIPS	United States Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
QCP	Qualified Certificate Policy
QCP+SSCD	Qualified Certificate Policy with Secure Signature Creation Device
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
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
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
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
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://www.harica.gr. Distributed repositories may exist for each Subordinate CA / Registration Authority that participates in the PKI.

2.2 Disclosure of Certification Authority

HARICA maintains a repository accessible through the Internet in which it publishes the Digital Certificate of the Root Certification Authority (type X.509v3), the Digital Certificates that are issued according to the Certification Practice Statement, the current CRL, the document of Certification 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.

Moreover, the search of certificates and CRLs is possible using the directory service of HARICA or that of the Externally Operated Subordinate CAs.

HARICA conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published at http://www.cabforum.org. HARICA also conforms to the current version of the "Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" published at https://aka.ms/csbr. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document. This means that HARICA will continuously keep track of changes in CA/B Forum Baseline Requirements and https://aka.ms/csbr and incorporate the changes before their effective dates, and update this CP/CPS accordingly.

Software vendors may use the following web sites for User Agent Verification:

- https://www.harica.gr which provides a "valid" certificate
- https://revoked.harica.gr which provides a "revoked" certificate
- https://expired.harica.gr which provides an "expired" certificate.

2.3 Frequency of publication

The certificates issued by HARICA are being published immediately after their retrieval from the Subscriber according to section 4.4.2.

CRLs are updated according to section 0.

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 names that are used for certificate issuance depend on the class of the certificate and they are per the 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. 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 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
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
OrganizationIdentifier (OID: 2.5.4.97)	A unique identifier for the Organization

3.1.4.1 End-Entity Certificates and Qualified Certificates for electronic signatures

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

- "Common Name"
- "GivenName" and "Surname"
- "Country"

3.1.4.2 End-Entity Certificates and Qualified Certificates for electronic seals

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

- "Common Name"
- "Organization"
- "Country"
- "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) 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 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:

- "Common Name"
- "Organization"
- "Country"
- "Locality" or "stateOrProvinceName"

3.1.4.4 End-Entity Certificates for Code Signing

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

- "Common Name"
- "Organization". 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
- "Country"
- "organizationIdentifier"

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

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.

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.

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).

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 on behalf of a Legal Entity (under the QCP-l or QCP-l-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.

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:

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

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/Tradename/Roles

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

If the 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 confirms that, as of the date the Certificate was issued, either HARICA or a Delegated Third Party has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed in this sub-section 3.2.2.4.

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 period of time specified in the relevant requirement (such as defined 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, or Affiliate.

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***

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

- HARICA authenticates the Applicant's identity under Section 3.2.2.1 and the authority of the Applicant Representative under Section 3.2.5, OR
- HARICA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

*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 or a Delegated Third Party 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 or a Delegated Third Party 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 30 days from its creation.

*3.2.2.4.3 **[Reserved]***

*3.2.2.4.4 **Constructed Email to Domain Contact***

Confirm the Applicant's control over the requested FQDN by

(i) 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,
(ii) including a Random Value in the email, and
(iii) 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 30 days from its creation.

*3.2.2.4.5 **Domain Authorization Document***

Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. HARICA MUST verify that the Domain Authorization Document was either

(i) dated on or after the date of the domain validation request or

(ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

*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 in the content of a file or on a web page in the form of a meta tag one of the following 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 HARICA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request for the file or web-page.

If a Random Value is used, HARICA or a Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of

(i) 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).

*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 TXT record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, HARICA or Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after

(i) 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).

*3.2.2.4.8 **[Reserved]***

*3.2.2.4.9 **[Reserved]***

3.2.2.4.10 ***[Reserved]***

3.2.2.5 Authentication for an IP Address

Not applicable according to 3.1.1.1.

3.2.2.6 Wildcard Domain Validation

HARICA does not currently issue certificates containing a wildcard character (*).

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.

3.2.2.8 CAA Records

HARICA must check for a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found.

CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA as set out in section 7.1.5.

CAA checking is optional 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.

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 Secure Signature Creation Device

(SSCD) or 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 SSCD/QSCD. Possible Policy Identifiers for "Class A" Certificates are:

- NCP+
- QCP+ (a.k.a. QCP-sscd)
- QCP-n-qscd
- QCP-l-qscd

"Class B" refers to certificates whose private keys are generated using software (software certificate store). Regardless of certificate "Class", an identification of the Applicant with her/his physical presence and an acceptable official document proving the physical identity, always takes place. Possible Policy Identifiers for "Class A" Certificates are:

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

The Central Registration Authority may also rely on the control of identity performed by 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 by means of an official document that bears the photograph of the beneficiary (e.g. police identity, passport, driving license, student identity card) and which is considered reliable by the familiar institution. 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 e-mail address), there is no need to repeat the procedure but a typical confirmation through the officially certified e-mail address of the user is considered sufficient. All requirements of section 4.2.1 apply.

HARICA's Central RA uses the following methods for identity, e-mail ownership and control verification:

i. Simple e-mail verification. The Applicant enters the e-mail address at the initial certificate request form and a verification e-mail is sent back with a link to a unique web page. After following this link, an e-mail 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 e-mail. 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 e-mail account) then there is no reason to be repeated.
ii. LDAP server. The Applicant enters the personal e-mail 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 e-mail 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 e-mail address by performing a challenge-response procedure according to "Simple e-mail 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, for Qualified Certificates for electronic signatures and Qualified Certificates for electronic seals they MUST include the OID id-etsi-qcs-QcSSCD at the qcStatements extension. Class A certificates are fully compliant with the Secure Signature Creation Device (SSCD) and Qualified Signature/Seal Creation Devices (QSCD) definition, per Precedential Decree 150/2001 and EU Regulation 910/2014.

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

3.2.3.2 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 e-mail 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 abovementioned 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.

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 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, fifteen (15) days 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 e-mail addresses.

The entire revocation process is described in section 4.9.3.

3.4.1 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 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 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 application

Applications for certificate issuance may be submitted by Applicants as described in section 1.3.3.

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, if 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 request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all information contained therein is correct

Applicants may submit a certificate application request through a secure web interface https://www.harica.gr/, or through the registration office of her/his own institution, or through HARICA's Central RA. The application process will result in the secure submission of a properly formatted CSR.

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 than thirty-nine (39) months 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 digital application contains faults, the application is rejected.

HARICA may reject a request for any certificate the issuance of which may harm, diminish or otherwise negatively impact HARICA PKI, 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.

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

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)

Effective as of **8 September 2017**, HARICA shall review CAA records as defined in RFC6844 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.

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 e-mail. In the same e-mail message, if the application is accepted, a unique URL is sent to the Applicant who MUST additionally accept the terms and services of HARICA before accepting and receiving the issued certificate, thus becoming a Subscriber.

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 MUST declare on the secure webpage that they have checked all certificate elements and that they are correct, to retrieve their certificate. Finally, they 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 e-mail messages using the S/MIME protocol
- Encryption of e-mail 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 **five (5) years** for client certificates and **three (3) years** for server certificates. If the Subscriber revokes a Certificate (for any 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 a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing or via a designated portal by using the certificate revocation code, 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 Certificates for electronic seals where there is a change in Legal representation and the former Legal representative is no longer authorized to create Advanced 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 no longer complies with the technical requirements described in sections 6.1.5 and 6.1.6.
4. HARICA obtains evidence that the Certificate was misused
5. HARICA is made aware that a Subscriber has violated one or more of its obligations under the Subscriber or Terms of Use Agreement
6. 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.

7. [reserved]
8. HARICA is made aware of a material change in the information contained in the Certificate
9. HARICA is made aware that the Certificate was not issued in accordance with this CP/CPS
10. HARICA determines that any of the information appearing in the Certificate is inaccurate or misleading
11. HARICA ceases operations for any reason and has not planned for another CA to provide revocation support for the Certificate
12. HARICA's right to issue Certificates expires or is revoked or terminated, unless HARICA has planned to continue maintaining the CRL/OCSP Repository
13. HARICA is made aware of a possible compromise of the Private Key that signed the Certificate
14. Revocation is required by HARICA's Certificate Policy and/or Certification Practice Statement or
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

HARICA shall revoke a Subordinate CA Certificate 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 Externally Operated Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has planned to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the Subordinate CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Subordinate CA Certificates should be revoked and replaced by CAs within a given period).

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 subject of the certificate 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 revocation request via e-mail to ca 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 Certification 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.

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

HARICA must begin the investigation of a Certificate Problem Report within **one (1)** business day except from force majeure cases.

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, at least every **single (1) day**. The CRL will be in effect for a maximum time of **seven (7) days**.
- 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 RFC6960. 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 RFC6960.

4.9.10 Online revocation checking requirements

HARICA supports OCSP capability using the GET method.

- For the status of Subscriber Certificates: HARICA SHALL update information provided via an Online Certificate Status Protocol at least every **eight (8) hours**. OCSP responses from this service MUST have a maximum expiration time of **two (2) days**.
- 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.

Relying Parties MUST follow the procedures described in section 1.3.4 before relying on any certificate. Before trusting a certificate, they must also check the OCSP responder and inquire the status of all Subordinate CA Certificates that chain to a HARICA ROOT CA Certificate. The URL of the OCSP service is included in all issued certificates.

4.9.11 Other forms of revocation advertisements available

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

4.9.12 Special requirements re-key compromise

As defined in section 4.9.1.

4.9.13 Circumstances for suspension

Certificate suspension is not provided.

4.9.14 Who can request suspension

Certificate suspension is not provided.

4.9.15 Procedure for suspension request

Certificate suspension is not provided.

4.9.16 Limits on suspension period

Certificate suspension is not provided.

4.10 Certificate status services

4.10.1 Operational characteristics

Revocation entries on a CRL or OCSP Response shall not be removed until after the Expiry Date of the revoked Certificate.

4.10.1.1 Online Certificate status service OCSP

As defined in section 4.9.10.

4.10.1.2 Online Certificate Repository

The 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.

4.10.1.3 Usage of Certificate Revocation Lists (CRL)

As defined in section 4.9.6.

4.10.2 Service Availability

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

HARICA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to competent public authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional features

Not defined.

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

Not defined.

4.12.2 Session key encapsulation and recovery policy and practices

Not defined.

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.

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.

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.

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

Not defined.

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.

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. All servers that record logs are synchronized via NTP (Network Time Protocol) as described in section 6.8.

5.4.2 Frequency of processing log

All transactions are archived daily.

5.4.3 Retention period for audit log

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.

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.

5.4.4.1 Access

Access to the transaction files is allowed only for reading to certain CA/RA applications and to authorized personnel.

5.4.4.2 Protection against changes in transactions file

An access policy is applied that allows changes only to the administrators of the operating system of the CA and the RA software.

5.4.4.3 Protection against deletions in transactions file

An access policy is applied that allows changes only to the administrators of the operating system of the CA and the RA software.

5.4.5 Audit log backup procedures

A backup of the transactions-events file is kept.

5.4.6 Audit collection system (internal vs. external)

Not defined.

5.4.7 Notification to event-causing subject

Not defined.

5.4.8 Vulnerability assessments

HARICA performs periodic Penetration Tests, at least annually, and quarterly Vulnerability Scans 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 retail records relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least

- **thirty (30) 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

Not defined.

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

Not defined.

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 RFC3161) 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)

Not defined.

5.5.7 Procedures to obtain and verify archive information

Not defined.

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. 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 of private key compromise of a Certification Authority, 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.

Following a disaster, appropriate measures should be 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 plan will be created. 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 per this CP/CPS. After the transfer of services, CA private keys, including backup copies, shall be destroyed or withdrawn from use.

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 after any Certificate based on that documentation ceases to be valid to be available for any lawful control. 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

Applicant keys are generated by hardware and software at the Applicant's side and remain under their absolute 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.

Especially, in case an Applicant wishes to obtain a "Class A" certificate, as described in section 3.2.3.1 she/he must submit the application under the presence of an authorized person of the Registration Authority to certify the key generation takes place in a crypto-token hardware device as defined in section 6.2.1.

CA keys 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 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 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.

6.1.2 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.

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.

Especially for the issuance of Qualified Certificates in Secure Signature Creation Devices (QCP+SSCD) or Qualified Certificates in Qualified Signature/Seal Creation Devices (QCP-n+QSCD, QCP-l+QSCD), IT IS FORBIDDEN TO PERFORM A KEY GENERATION OPERATION WITHOUT THE ABSOLUTE CONTROL OF THE SUBSCRIBER.

6.1.3 Public key delivery to certificate issuer

The Applicant must submit the public key to the Registration Authority through a structured application (e.g. format PKCS#10) for certificate issuance. The 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 snail mail delivery and transmission of the corresponding fingerprints via an alternative communication channel.

6.1.5 Key sizes

The minimum allowed key size for a Subscriber is 2048 bits RSA or ECC equivalent P256 for all cases (e.g. code-signing or timestamping certificates). Effective Jan 1 2016, CAs that issue certificates with the codeSigning extended key usage set, MUST chain up to a ROOT CA with a minimum of RSA 4096-bit modulus or ECC equivalent (P384) and MUST support the SHA2 hash algorithms.

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. CA private keys are generated using secure algorithms and parameters based on current research and industry standards.

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 a software security device or a hardware cryptographic module. In the special case of Qualified Certificates with Secure Signature Creation Device (SSCD), or Qualified Signature/Seal Creation Device (QSCD) (Class A certificates), the private key MUST be generated and stored in a SSCD or QSCD and cannot be extracted in any form. SSCD and 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.

In case an SSCD or QSCD fails to maintain its certification, the proper regulatory authorities will alert QTSPs to stop using certain devices. Independently, HARICA also monitors relevant information for SSCD/QSCD certifications.

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

Not defined.

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.

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 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 also 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 that relates to a ROOT CA, 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

Not defined.

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 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 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 is defined by the operational period of the corresponding digital certificate. The maximum operational period of the keys 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 or S/MIME Certificates, **two (2) years** for SSL/TLS and Code Signing Certificates **ten (10) years** for a Time-Stamping Unit 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.

6.4 Activation data

6.4.1 Activation data generation and installation

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.

6.4.2 Activation data protection

Not defined.

6.4.3 Other aspects of activation data

Not defined.

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.

6.5.2 Computer security rating

Not defined.

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 PKI follows the network security guidelines of section 7.4 of the ETSI TS 102 042.

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

The connection of CA software to wider data networks or other telecommunication media (e.g. the telephone network using a modem) is not allowed. The Registration

Authority is protected from the internet using strong security mechanisms including firewalls. 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 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 RFC5280 "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile" is used.

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 *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

- 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 Alternative Name (required for SSL/TLS Certificates): It provides multiple values for e-mail 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)

  This list of values is not limited. Additionally, **it is forbidden** for Issuing CAs to issue Certificates **with both** the serverAuth and codeSigning extended key usages. **Effective January 1 2017**, a single Issuing CA must not be used to issue certificates that blend the serverAuth, the emailProtection the codeSigning and the timestamping extended key usages. After this effective date, new Issuing CAs must separate Server Authentication, S/MIME, Code Signing and Time Stamping Extended Key Usages.
- Qualified Certificate Statements (qcStatements): It provides one or more values that specify the attributes of the Certificate for electronic signatures/seals. The value "`id-etsi-qcs-QcCompliance`" specifies that the certificate is a Certificate for electronic signatures/seals per Regulation (EU) No. 910/2014 MUST always be present. Additionally, Qualified Certificates for electronic signatures/seals MUST include the value "`id-etsi-qcs-QcSSCD`", which asserts that the private key was generated in an SSCD/QSCD.

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 section 6.1.5. 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.

7.1.4 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 7.1.1.3.

7.1.4.4 Issuer

The issuer information contains:

- Common Name (CN) (Optional if there is Issuing OU): Issuing Authority Common Name.
- Organizational Unit (OU) (Optional if there is Issuing CN): Issuing Certification Authority.
- Organization (O): Organization Name
- Country (C): Issuing Country.

The issuer DN must be unique in the HARICA PKI.

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 begins (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) (Optional for SSL/TLS certificates): The e-mail address of the subject as verified under section 3.2.2.4.2.
- Common Name (OID: 2.5.4.3) (Optional for SSL certificates, Required for Code Signing and Client Certificates): Subject Common Name. If present, for SSL/TLS certificates, this field MUST contain an FQDN 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.
- Organizational Unit (OU) (Optional): Subject Organizational Unit or sub-unit, or special attribute of the signatory depending on the intended use or attributes of the certificate.
- Organization (OID: 2.5.4.10): Subject Organization Name as verified under section 3.2.2.1
- Locality (OID: 2.5.4.7) (Optional if "State or Province" is present): Subject Locality as verified under section 3.2.2.1
- State or Province (OID: 2.5.4.8) (Optional if "Locality" is present): Subject State as verified under section 3.2.2.1
- Country (OID: 2.5.4.6): Subject Country as verified under section 3.2.2.1
- 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) (Optional): 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: "**PNO**GR-12345678". In this example, GR is the Subject's Country.
    - Personal Identification Card with the following semantics: "**IDC**GR-AK1234567". In this example, GR is the Subject's Country.
    - Tax Identification Number with the following semantics: "**TIN**EL-123456789". Especially for Tax Identifiers, the "country" identifier value should comply with the European Council Directive 2006/112/EC article 215. In this example, EL is the Subject's Country for Greece.
    - Passport Number with the following semantics: "**PAS**GR-1231232". In this example, GR is the Subject's Country.
    - A Unique 10-digit Identifier assigned by HARICA
- OrganizationIdentifier (OID: 2.5.4.97): Per QCP-l and QCP-l-qscd, contains a unique identifier for the Organization per ETSI EN 319 412-3. Depending on the Legal Entity's decision, one of the following identifiers must be used:

- Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**GR-123456789". In this example, GR is the Subject's Country.
- Legal Entity's Tax Identification Number with the following semantics: "**VAT**EL-123456789". Especially for Tax Identifiers, the "country" identifier value should comply with the European Council Directive 2006/112/EC article 215. In this example, EL is the Subject's Country for Greece.

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.

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 (2.5.4.42) and surname (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 electronic signatures under the QCP-n policy or a Qualified Certificate for 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 electronic seals under the QCP-l policy or a Qualified Certificate for electronic seals under the QCP-l-qscd policy, HARICA shall include at least the "commonName", "Country", "organizationName" and "OrganizationIdentifier" attributes in the SubjectDN field.

7.1.5 Name constraints

HARICA uses the name constraints extension per RFC5280, 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 1.3.6.1.4.1.**26513.1.0.3.5**. According to each certificate class, the following recognized OIDs can be added in the certificatePolicies extension:

- **BTSP** (Best practice policy for time-stamp) as specified in ETSI EN 319 421: OID **0.4.0.2023.1.1**
- **QCP-n** as described in ETSI EN 319 411-2: OID **0.4.0.194112.1.0**
- **QCP-l** as described in ETSI EN 319 411-2: OID **0.4.0.194112.1.1**
- **QCP-n-qscd** as described in ETSI EN 319 411-2: OID **0.4.0.194112.1.2**
- **QCP-l-qscd** as described in ETSI EN 319 411-2: OID **0.4.0.194112.1.3**
- QCP Public+SSCD (**QCP+**) as described in ETSI TS 101 456: OID **0.4.0.1456.1.1**
- QCP Public (**QCP**) as described in ETSI TS 101 456: OID **0.4.0.1456.1.2**
- **NCP** (Normalized Certificate Policy) as described in ETSI TS 102 042 and ETSI EN 319 411-1: OID **0.4.0.2042.1.1**
- **NCP+** (Extended Normalized Certificate Policy) as described in ETSI TS 102 042 and ETSI EN 319 411-1: OID **0.4.0.2042.1.2**

- **DVCP** (Domain Validated Certificate Policy) as described in ETSI TS 102 042 and ETSI EN 319 411-1: OID **0.4.0.2042.1.6**
- **OVCP** (Organizational Validation Certificate Policy) as described in ETSI TS 102 042 and ETSI EN 319 411-1: OID **0.4.0.2042.1.7**
- **Code Signing** as described in section 9.3.1 of the https://aka.ms/csbr: OID **2.23.140.1.4.1**

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.

7.1.7 Usage of Policy Constraints extension

Not defined.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifier is the URI which points to the published HARICA CP/CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not defined.

7.2 CRL Profile

7.2.1 Basic CRL Contents

7.2.1.1 Version number

The version number is 1 or/and 2, which corresponds to CRL X.509v2, following RFC5280.

7.2.1.2 Signature Algorithm

The signature algorithm MUST use a hashing algorithm from the SHA2 family or stronger.

7.2.1.3 Issuer

The Distinguished Name of the Certification Authority that has signed and issued the CRL.

7.2.1.4 This Update

Issue date of the CRL in GMT.

7.2.1.5 Next Update

Date by which the next CRL shall be issued in GMT. The requirements of section 4.9.7 apply.

If a Subordinate CA:

1. issues Client Certificates used for document or code signing purposes and
2. all these certificates are either expired or revoked and

3. this Subordinate CA stops issuing new Certificates

then this Subordinate CA may generate the last CRL issued for those certificates in the scope of the 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.

7.2.1.6 Revoked Certificates

List of all revoked certificates including their serial number and the date and time of the revocation in GMT.

7.2.2 CRL and CRL entry extensions

Not defined.

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 RFC6960.

7.3.1 Version number

Version 1 of the OCSP specification as defined by RFC6960 is supported.

7.3.2 OCSP extensions

The OCSP service uses a secure timestamp and a maximum validity period of 2 days 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 nonce extension is supported by the OCSP responder. Requests containing a nonce should use it to verify the freshness of the response. Otherwise, the local clock and the timestamp contained in the response should be used.

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*",
- ETSI TS 101 456 "*Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates*",
- ETSI TS 102 042 standard *"Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*,
- Precedential Decree 150/2001 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 "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document, produced by the CA/Browser Forum (www.cabforum.org).

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 current 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 use.

During the period in which a Technically Constrained Subordinate CA issues Certificates for SSL/TLS use, HARICA which signed the Subordinate CA Certificate SHALL monitor adherence to this CP/CPS.

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

Not defined.

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 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

Not defined.

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 Information disclosure to law enforcement and judicial agencies

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 there is an official court order according to the privacy and data protection applicable law. The process is carried out through the Management Committee of HARICA. Currently, HARICA is operated by GUnet S.A. Private keys used to sign and issue digital certificates are never disclosed to any third-parties, unless applicable law specifically demands disclosure.

9.4.6 Information disclosure available for entity queries

All non-classified and non-private information stored at the Certification and Registration Authorities is available for entity queries, once applied for.

9.4.7 Conditions for information disclosure to its owner

All information stored at the CA and RA is available to its rightful owner (e.g. individual who applied for a certificate), once applied for.

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, 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.

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 manages the applications.

- ✓ 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 e-mail, 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 e-mail 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 money transactions (e.g. credit-card payments via e-shop) or for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger of life.
- ✓ 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 malware 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 money transactions (e.g. credit-card payments via e-shop) or 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

Not defined

9.7 Disclaimers of warranties

Not defined

9.8 Limitations of liability

This clause applies to liability under contract (including under any indemnity or breach of warranty), in tort (including negligence), under statue or otherwise for non – compliant usage of the certificate(s) the associated private keys, the revocation status information or any other hardware or software provided, and any consequential, incidental, special, or exemplary damages arising out of or related to this CP/CPS, including but not limited to, loss of data, loss of business and loss of profit. Except as set out in the next paragraph, and to the extent permitted by applicable law, HARICA cannot and shall not be held liable for any problems or damages that may arise from its services in case of wrongful, negligent or improper use of the issued certificates. HARICA does not undertake any financial, civil or other responsibilities for such cases. Using HARICA and its certification services requires that users unconditionally accept the terms and services of this CP/CPS and that HARICA is not liable and does not undertake any financial, civil or

other responsibilities, except for cases where there is evidence of fraudulent intent or serious negligence by HARICA or its operators. HARICA shall not be liable to the Subscriber for any loss suffered by the Subscriber due to use of a Certificate outside the normal and intended use. Subscribers are obliged to request Certificate revocation for reasons stated in section 9.6.3. Failure to request revocation of the Certificate, voids any liability claims if the private key or the Certificate is mis-used, when it should have been revoked with actions originating from the Subscriber.

In the event that HARICA deviates from the provisions set forth in this CP/CPS when issuing "**Qualified Certificates for electronic signatures**" and "**Qualified Certificates for electronic seals**", certain liability provisions apply:

- HARICA is only liable for the correct verification of the application and the resultant contents of Qualified Certificates (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 Qualified 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 Qualified Certificate or if the Subscriber uses the Qualified Certificate in an incorrect way.
- With the exception of the previous cases, HARICA's maximum aggregate liability under this CP/CPS sustained by the Subscribers is limited to a maximum of 1.000€ per Certificate for Qualified Signatures/Seals 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 for Qualified Signatures/Seals, 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 Insurance contract between HARICA and a major Insurance Company.

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, information provided by the Subscriber or Subscriber's or its customers' infringement on the rights of a third party.

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 Certification Policy and to the Certification Practice Statement without any prior notice and without OID modification.

9.12.2 Notification mechanism and period

In case of major 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 major document changes. The most recent CP/CPS is always published at the following URL: http://www.harica.gr/documents/CPS.php.

9.12.3 Circumstances under which OID must be changed

In case of major and significant changes of the CP/CPS, the name and identifier (OID) which is reported in section 1.2 will be altered. Subscribers will be informed beforehand in case of important changes in the Certification Policy.

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 Certification 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 Certification 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 Certification 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

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
         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:c9:4f: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:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

```
        Modulus:
            00:c2:f8:a9:3f:1b:89:fc:3c:3c:04:5d:3d:90:36:
            b0:91:3a:79:3c:66:5a:ef:6d:39:01:49:1a:b4:b7:
            cf:7f:4d:23:53:b7:90:00:e3:13:2a:28:a6:31:f1:
            91:00:e3:28:ec:ae:21:41:ce:1f:da:fd:7d:12:5b:
            01:83:0f:b9:b0:5f:99:e1:f2:12:83:80:4d:06:3e:
            df:ac:af:e7:a1:88:6b:31:af:f0:8b:d0:18:33:b8:
            db:45:6a:34:f4:02:80:24:28:0a:02:15:95:5e:76:
            2a:0d:99:3a:14:5b:f6:cb:cb:53:bc:13:4d:01:88:
            37:94:25:1b:42:bc:22:d8:8e:a3:96:5e:3a:d9:32:
            db:3e:e8:f0:10:65:ed:74:e1:2f:a7:7c:af:27:34:
            bb:29:7d:9b:b6:cf:09:c8:e5:d3:0a:fc:88:65:65:
            74:0a:dc:73:1c:5c:cd:40:b1:1c:d4:b6:84:8c:4c:
            50:cf:68:8e:a8:59:ae:c2:27:4e:82:a2:35:dd:14:
            f4:1f:ff:b2:77:d5:87:2f:aa:6e:7d:24:27:e7:c6:
            cb:26:e6:e5:fe:67:07:63:d8:45:0d:dd:3a:59:65:
            39:58:7a:92:99:72:3d:9c:84:5e:88:21:b8:d5:f4:
            2c:fc:d9:70:52:4f:78:b8:bd:3c:2b:8b:95:98:f5:
            b3:d1:68:cf:20:14:7e:4c:5c:5f:e7:8b:e5:f5:35:
            81:19:37:d7:11:08:b7:66:be:d3:4a:ce:83:57:00:
            3a:c3:81:f8:17:cb:92:36:5d:d1:a3:d8:75:1b:e1:
            8b:27:ea:7a:48:41:fd:45:19:06:ad:27:99:4e:c1:
            70:47:dd:b5:9f:81:53:12:e5:b1:8c:48:5d:31:43:
            17:e3:8c:c6:7a:63:96:4b:29:30:4e:84:4e:62:19:
            5e:3c:ce:97:90:a5:7f:01:eb:9d:e0:f8:8b:89:dd:
            25:98:3d:92:b6:7e:ef:d9:f1:51:51:7d:2d:26:c8:
            69:59:61:e0:ac:6a:b8:2a:36:11:04:7a:50:bd:32:
            84:be:2f:dc:72:d5:d7:1d:16:47:e4:47:66:20:3f:
            f4:96:c5:af:8e:01:7a:a5:0f:7a:64:f5:0d:18:87:
            d9:ae:88:d5:fa:84:c1:3a:c0:69:28:2d:f2:0d:68:
            51:aa:e3:a5:77:c6:a4:90:0e:a1:37:8b:31:23:47:
            c1:09:08:eb:6e:f7:78:9b:d7:82:fc:84:20:99:49:
            19:b6:12:46:b1:fb:45:55:16:a9:a3:65:ac:9c:07:
            0f:ea:6b:dc:1f:2e:06:72:ec:86:88:12:e4:2d:db:
            5f:05:2f:e4:f0:03:d3:26:33:e7:80:c2:cd:42:a1:
            17:34:0b
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            71:15:67:C8:C8:C9:BD:75:5D:72:D0:38:18:6A:9D:F3:71:24:54:0B
Signature Algorithm: sha256WithRSAEncryption
    75:bb:6d:54:4b:aa:10:58:46:34:f2:62:d7:16:36:5d:08:5e:
    d5:6c:c8:87:bd:b4:2e:46:f2:31:f8:7c:ea:42:b5:93:16:55:
    dc:a1:0c:12:a0:da:61:7e:0f:58:58:73:64:72:c7:e8:45:8e:
```

dc:a9:f2:26:3f:c6:79:8c:b1:53:08:33:81:b0:56:13:be:e6:
51:5c:d8:9b:0a:4f:4b:9c:56:53:02:e9:4f:f6:0d:60:ea:4d:
42:55:e8:7c:1b:21:21:d3:1b:3a:cc:77:f2:b8:90:f1:68:c7:
f9:5a:fe:fa:2d:f4:bf:c9:f5:45:1b:ce:38:10:2a:37:8a:79:
a3:b4:e3:09:6c:85:86:93:ff:89:96:27:78:81:8f:67:e3:46:
74:54:8e:d9:0d:69:e2:4a:f4:4d:74:03:ff:b2:77:ed:95:67:
97:e4:b1:c5:ab:bf:6a:23:e8:d4:94:e2:44:28:62:c4:4b:e2:
f0:d8:e2:29:6b:1a:70:7e:24:61:93:7b:4f:03:32:25:0d:45:
24:2b:96:b4:46:6a:bf:4a:0b:f7:9a:8f:c1:ac:1a:c5:67:f3:
6f:34:d2:fa:73:63:8c:ef:16:b0:a8:a4:46:2a:f8:eb:12:ec:
72:b4:ef:f8:2b:7e:8c:52:c0:8b:84:54:f9:2f:3e:e3:55:a8:
dc:66:b1:d9:e1:5f:d8:b3:8c:59:34:59:a4:ab:4f:6c:bb:1f:
18:db:75:ab:d8:cb:92:cd:94:38:61:0e:07:06:1f:4b:46:10:
f1:15:be:8d:85:5c:3b:4a:2b:81:79:0f:b4:69:9f:49:50:97:
4d:f7:0e:56:5d:c0:95:6a:c2:36:c3:1b:68:c9:f5:2a:dc:47:
9a:be:b2:ce:c5:25:e8:fa:03:b9:da:f9:16:6e:91:84:f5:1c:
28:c8:fc:26:cc:d7:1c:90:56:a7:5f:6f:3a:04:bc:cd:78:89:
0b:8e:0f:2f:a3:aa:4f:a2:1b:12:3d:16:08:40:0f:f1:46:4c:
d7:aa:7b:08:c1:0a:f5:6d:27:de:02:8f:ca:c3:b5:2b:ca:e9:
eb:c8:21:53:38:a5:cc:3b:d8:77:37:30:a2:4f:d9:6f:d1:f2:
40:ad:41:7a:17:c5:d6:4a:35:89:b7:41:d5:7c:86:7f:55:4d:
83:4a:a5:73:20:c0:3a:af:90:f1:9a:24:8e:d9:8e:71:ca:7b:
b8:86:da:b2:8f:99:3e:1d:13:0d:12:11:ee:d4:ab:f0:e9:15:
76:02:e4:e0:df:aa:20:1e:5b:61:85:64:40:a9:90:97:0d:ad:
53:d2:5a:1d:87:6a:00:97:65:62:b4:be:6f:6a:a7:f5:2c:42:
ed:32:ad:b6:21:9e:be:bc

=== END HARICA ROOT CA 2015 ===

=== BEGIN HARICA ECC ROOT CA 2015 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions ECC RootCA 2015
        Validity
            Not Before: Jul  7 10:37:12 2015 GMT
            Not After : Jun 30 10:37:12 2040 GMT
        Subject: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions ECC RootCA 2015
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:92:a0:41:e8:4b:82:84:5c:e2:f8:31:11:99:86:
                    64:4e:09:25:2f:9d:41:2f:0a:ae:35:4f:74:95:b2:
```

```
            51:64:6b:8d:6b:e6:3f:70:95:f0:05:44:47:a6:72:
            38:50:76:95:02:5a:8e:ae:28:9e:f9:2d:4e:99:ef:
            2c:48:6f:4c:25:29:e8:d1:71:5b:df:1d:c1:75:37:
            b4:d7:fa:7b:7a:42:9c:6a:0a:56:5a:7c:69:0b:aa:
            80:09:24:6c:7e:c1:46
        ASN1 OID: secp384r1
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            B4:22:0B:82:99:24:01:0E:9C:BB:E4:0E:FD:BF:FB:97:20:93:99:2A
Signature Algorithm: ecdsa-with-SHA256
    30:64:02:30:67:ce:16:62:38:a2:ac:62:45:a7:a9:95:24:c0:
    1a:27:9c:32:3b:c0:c0:d5:ba:a9:e7:f8:04:43:53:85:ee:52:
    21:de:9d:f5:25:83:3e:9e:58:4b:2f:d7:67:13:0e:21:02:30:
    05:e1:75:01:de:68:ed:2a:1f:4d:4c:09:08:0d:ec:4b:ad:64:
    17:28:e7:75:ce:45:65:72:21:17:cb:22:41:0e:8c:13:98:38:
    9a:54:6d:9b:ca:e2:7c:ea:02:58:22:91
```

=== END HARICA ECC ROOT CA 2015 ===

11 ANNEX B (HARICA Common Certificate Profiles)

Friendly Name	Policy IDs	Key Usages	Other Extensions
HARICA Internally Operated Subordinate CACertificate	**2.5.29.32.0 (anyPolicy)** or the CP/CPS OID in case of externally operated CA	KU: **Certificate Signing, CRL Signing** EKU: None	None
OCSP Certificate	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature** EKU: **OCSP Signing**	**OCSP No Check**
Client Certificate	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2042.1.1 (NCP)**	KU: **Digital Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, Email Protection,** Encrypting File System (optional)	None
Qualified User Certificate	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.1456.1.2 (QCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment**1 EKU: **TLS Web Client Authentication, Email Protection**	**QcStatements:** `id-etsi-qcs-QcCompliance`

Qualified User Certificate in Secure Signature Creation Device	**1.3.6.1.4.1.26513.1.0.3.5**
	0.4.0.1456.1.1 (QCP+)
		KU: **Non Repudiation, Digital Signature**
		EKU: **TLS Web Client Authentication, Email Protection, Smart Card Logon** (optional)
			QcStatements:
			`id-etsi-qcs-QcCompliance,`
			`id-etsi-qcs-QcSSCD`
			SmartcardUser (optional)

Certificate for electronic signatures	**1.3.6.1.4.1.26513.1.0.3.5**
	0.4.0.194112.1.0 (QCP-n)
		KU:**Digital Signature, Key Encipherment**[1]
		EKU: **TLS Web Client Authentication, Email Protection, Document Signing**
			QcStatements:
			`id-etsi-qcs-QcCompliance,`
			`id-etsi-qcs-QcPDS,`
			`id-etsi-qct-esign,`
			`id-etsi-qcs-SemanticsId-Natural(optional)`

[1] "Key Encipherment" is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.

Qualified Certificate for electronic signatures	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.194112.1.2 (QCP-n-qscd)**	KU: **Non Repudiation, Digital Signature** EKU: **TLS Web Client Authentication, Email Protection, Document Signing**	**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)
Certificate for electronic seal	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.194112.1.1 (QCP-l)**	KU: **Digital Signature** EKU: **TLS Web Client Authentication, Email Protection, Document Signing**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(optional)
Qualified Certificate for electronic seal	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.194112.1.3 (QCP-l-qscd)**	KU: **Non Repudiation, Digital Signature** EKU: **TLS Web Client Authentication, Email Protection, Document Signing**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(optional)
Time stamping	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2023.1.1(BTSP)**	KU: **Digital Signature** EKU:**Time Stamping**	None
Qualified Time stamping	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2023.1.1(BTSP)**	KU: **Non Repudiation, Digital Signature** EKU:**Time Stamping**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS
Code Signing	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2042.1.1 (NCP)** **2.23.140.1.4.1**	KU: **Digital Signature** EKU: **Code Signing, Lifetime Signing**	None

Code Signing Certificate in Secure Signature Creation Device	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2042.1.2 (NCP+)** **2.23.140.1.4.1**	KU: **Digital Signature** EKU:**Code Signing, Lifetime Signing**	None
DV SSL/TLS Certificate	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2042.1.6 (DVCP)**	KU: **Digital Signature, Key Encipherment**1 EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None
OV SSL/TLS Certificate	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature, Key Encipherment**1 EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None
OV SSL/TLS Enhanced Device Certificate	**1.3.6.1.4.1.26513.1.0.3.5** **0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature, Key Encipherment**1 EKU: **TLS Web Client Authentication, TLS Web Server Authentication, IPSec End System, IPSec Tunnel, IPSec User**	None