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 3.3 (March 17th 2016)

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 2.2Adapt 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)

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 Certification Services Provider (CSP). 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 the previously mentioned Memorandum.

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.

The HARICA Certification Authority issues User Certificates, Network Device Certificates (e.g. Servers, routers etc.) and Subordinate Certification Authority Certificates. All certificates contain a reference to this document. 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 TS 101 456 v1.4.3. This audit is consistent with standards technical specification Electronic Signatures and Infrastructures (ESI); "Policy requirements for certification authorities issuing qualified certificates" under the scope QCP, QCP+SSCD.
- ETSI TS 102 042 v2.4.1. This audit is consistent with standards technical specification Electronic Signatures and Infrastructures (ESI); "Policy requirements for certification authorities issuing public key certificates" under the scope DVCP, OVCP.
- Qualified Certification Service Provider, following the Presidential Decree 150/2001 of the Hellenic Republic and Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.

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 frame of HARICA Public Key Infrastructure. In abbreviation, it will be refereed 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 RFC-3647 with the minimum necessary changes in order to reflect the particular needs of the Academic and research community. 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.

The globally unique Identification Number (OID) of this document is: 1.3.6.1.4.1.**26513.1.0.3.3** 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
3.3	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 Public Key Infrastructure constitute the community governed by this Certification Policy and Certification Practice Statement.

1.3.1 Certification Authorities

Certification Authorities (CAs) are the entities of the Public Key Infrastructure responsible for issuing certificates. Every Certification Authority utilizes one or more Registration Authorities (RAs). RAs provide the means of communication between the users and the corresponding Certification Authority.

The hierarchy of the Certification Services Provider is constituted by the following entities:

1. Root Certification Authorities (HARICA-ROOT-CA) which issue digital certificates exclusively for Subordinate Certification Authorities that may operate on behalf of other academic institutions or other organizations and does not issue certificates to end entities. As an exception, it is allowed to only issue a certificates for OCSP responders according to RFC2560 and draft-cooper-pkix-rfc2560bis-00.txt (see Figure 7 of the draft: "Designated OCSP Responder and CA with Two Keys Certified by Root CA"). The validity period of the HaricaRootCA2011 certificate is twenty (20) years and of the HaricaRootCA2015 and HaricaECCRootCA2015 is twenty five (25) years. If the root certificate is RSA 2048 bits, it should stop being used by year 2030. See ANNEX A (HARICA ROOTS) for information about HARICA Root CAs.
2. Subordinate Certification Authorities of HARICA under the control of the RootCA operators on behalf of organizations that comply with and fully adopt this Certification Policy and Certification Practice Statement. The validity period of the certificates of the Subordinate Certification Authorities is eight (8) to fifteen (15) years. SubCAs may be operated by an external Organization,

described in this document as "Externally Operated subCAs" which must be properly audited and technically constrained according to RFC5280 and according to policies set forth by the Root programs of Mozilla/Microsoft/Apple and comply with the Precedential decree 150/2001. In the case where a subordinate CA needs a different policy and practices or in the case of externally operated CAs, a separate CP/CPS document must be created (with a unique OID) and entered in the appropriate policy extension field of the corresponding subCA certificate.

3. HARICA may issue cross-certificates according to 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 the particular Certification Authority in a secure manner. GUnet is the central Registration Authority of HARICA and apply strict procedures for users' authentication.

1.3.3 Subscribers

PKI Subscribers are defined in section 1.6.1 and are entities who request and successfully acquire a digital certificate signed by HARICA or any subordinate CA.

The subscription of roles (e.g. 'Rector') 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 or simply 'users' of the certification services can be any entity, inside or outside the Hellenic academic community, 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 Provider (CSP) are the 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 the CSP of HARICA PKI, 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, the user must check that:

- √ The validity period of the certificate has begun and has not expired.
- √ The certificate is correctly signed by a Trusted Certification Authority.
- √ The certificate has not been revoked for any reason.
- √ Subject identification matches the details that the signer presents.
- √ The usage for which the certificate is presented and is according to the reason it was issued by HARICA.

√ Abides by the terms and the conditions that are described in the present Certification Practice Statement.

1.3.5 Other participants

Not specified.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The 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 the Certification Services Provider Service, can be used, are the following (the list is not restrictive):

a) Signing of an "electronic document" by a person using her/his digital certificate and the relevant private key, preferably with the use of a "Secure Signature Creation Device" SSCD (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 signer to the content of document and the non-repudiation of signature.

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

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

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

e) Certification of other Certificate Services Providers such as a Subordinate CA 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, IPSec etc.

1.4.2 Forbidden certificate use

Certificates cannot be used for money transactions (e.g. credit-card payments via e-shop) or any other transactions 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 and relying parties with due notice before they become effective. 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. 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 BR and incorporate the changes before their effective dates and update this CP/CPS accordingly.

Even if there are is no compulsory reason for a change in this CP/CPS, the PMC performs a management review 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

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 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 industry standards Requirements suitable for publicly Trusted Certificate Service Providers.

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 the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which 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. The term applies equally to both Roots CAs and Subordinate CAs.

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

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

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

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

Domain Authorization Document: Documentation provided by, or a CA'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 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 subCAs: Entities that are unaffiliated with HARICA, that have control over a pair of key / subCA.

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.

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 a CA Key Pair **.**

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.

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

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

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.

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 8.3 (Auditor Qualifications).

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.

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

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

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

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

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

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

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

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 which 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.

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

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

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

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

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

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
	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
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-Stamp Authority
URL	Uniform Resource Locator
X.509	ITU-T standard for Certificates and authentication framework

2 Publication and Repository

2.1 Repositories

HARICA PKI 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 Certification Authority / Registration Authority that participates in the PKI.

2.2 Disclosure of Certification Authority

The HARICA PKI maintains a repository accessible through the Internet in which it publishes the Digital Certificate of the Root Certification Authority (type X.509.v3), 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).

CAs perform all the necessary actions for the uninterrupted - as possible - availability of its repository.

The HARICA PKI repository address is https://repo.harica.gr.

Moreover, the storage and search of certificates and CRLs is possible using the directory service of HARICA or that of the externally-operated CAs.

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 4.9.7.

2.4 Access controls on repositories

The repository section containing the certificates is publically 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 according to the X.500 standard for Distinguished Names.

3.1.1.1 Certificate name compliance with Baseline Requirements

All names in SSL certificates that chain to a publicly trusted CA shall conform to the CA/Browser (CAB) Forum Baseline Requirements regarding internal server names and/or reserved IP addresses. 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 the user certificates must be related to the subscriber / recipient of the certificate. 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 to clearly identify a certificate as unique.

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).

3.1.4.1 User certificates

Regarding the user certificates, the field that includes the name of a user corresponds to the characteristic "CN", the e-mail to "E", the organization to "O" or/and "OU", the locality in which it is found to "L" and the country to "C".

3.1.4.2 Device certificates

For devices under the DVCP, only the name of the device certificate (FQDN DNS) must be included in the "Subject Alternative Name – SAN" extension. The "CN" 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.
For devices under the OVCP, in addition to the above fields, the following information is included:

- the name of the organization the device belongs to, at the ”O” and optionally ”OU” field,
- the locality is found at the ”L” field and
- the country the device is located, at the ”C” field.

3.1.5 Uniqueness of names

The Distinguished Name of a subscriber must be unique for the particular subCA, while it is desirable to be unique in the entire hierarchy of certification of HARICA.

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 HARICA PKI is the HARICA members General Assembly.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The identity of the subscriber is authenticated and a CSR is submitted that contains the public key of the corresponding private key.

For Qualified Certificates with Secure Signature Creation Device (SSCD), in accordance with European/Greek Electronic Signature law (QCP+), private keys are generated on Secure 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 on the SSCD. The presence of an RA authorized member can be skipped if there is a certified procedure that ensures by technical means, that the subscriber’s private key is created on the SSCD. The Certificate Holder is responsible for securing the SSCD with a Personal Identification Number (PIN).

3.2.2 Authentication of organization identity

The Registration Authority must confirm that the subscriber belongs to the Organization, the name of which is included in the certificate. 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, HARICA 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.

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 PKI does not allow certificate issuance for anonymous users. The certificate issuance for pseudonyms e.g. "Rector" 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.

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 Section 3.2.2.1.

3.2.2.4 Authorization by Domain Name Registrant

For each Fully-Qualified Domain Name listed in a Certificate, HARICA shall confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this section) has control over the FQDN by:

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;
2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;
3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;
4. Communicating with the Domain's administrator using an email address created by pre-pending "admin", "administrator", "webmaster", "hostmaster", or

"postmaster" in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;

5. Relying upon a Domain Authorization Document;
6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN; or
7. Using any other method of confirmation, provided that HARICA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the FQDN to at least the same level of assurance as those methods previously described.

If HARICA relies upon a Domain Authorization Document to confirm the Applicant's control over a FQDN, then the Domain Authorization Document MUST substantiate that the communication came from either the Domain Name Registrant (including any private, anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. HARICA MUST also verify that the Domain Authorization Document was either:

- dated on or after the certificate request date or
- used by HARICA to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate's issuance.

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.

3.2.2.5 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.

3.2.3 Authentication of individual person identity

3.2.3.1 Entity applying for a user certificate

The certificates of individuals that are issued by the HARICA PKI must be checked for identification. There are two classes of user certificates. Class A includes certificates whose private keys are generated and reside on a Secure Signature Creation Device (SSCD) and are issued under the presence of authorized personnel of the RA who verify that the private key is actually generated in the SSCD. Class B includes certificates whose private keys are generated using software (software certificate store). Note that there is a secure identification of the recipient with her/his physical presence and an acceptable official document proving the physical identity in both classes of certificates.

The Registration Authority relies on the control of identity performed by the institutions the subscriber belongs to and uses authentication ways of user identities that are available in the institutions in order to check the identity. The collaborating 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 RA of HARICA can execute the above process of applicant identification for any individual requesting a personal certificate.

In case the familiar institution of the user, according to its policy, has already performed a procedure of physical identity verification in the past (e.g. for the provision of a 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 sufficient.

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

i. Simple e-mail verification. The user enters the e-mail address at the initial certificate request form and a verification e-mail is sent to the user with a link to a unique web page. After following this link, an e-mail is sent to the institution's network operation center mail administrator that requires an approval based on the full name entered by the user and the user's email. This approval requires the identification of the user with his/her physical presence and an acceptable official document. If this procedure took place before (e.g. for the creation of an e-mail account) then there is no reason to be repeated.
ii. LDAP server. The user enters the personal e-mail address at the initial certificate request form and the corresponding password. This information is verified against the institution's LDAP server. If the verification is successful, the RA queries the real name of the user and creates the certificate request. 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 user enters the personal e-mail address at the initial request form and is then redirected to the appropriate web page of the Identity Provider. The Identity Provider verifies the user and returns the real name and the email address of the user as attributes to the Registration Authority. In order for a user to be verified 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 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, military 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.

It is recommended for Class A certificates to include an extra organizational unit (OU) in the subject field with the value "Class A – Private Key created and stored in hardware CSP". Additionally, they MUST include the OID id-etsi-qcs-QcSSCD at the qcStatements extension. Class A certificates are fully compliant with the Secure Signature Creation Devices (SSCD) definition, according to Precedential Decree 150/2001. Certificates of Class B are recommended 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 individual who is in control of a device/server, either possesses a certificate issued by a CA that conforms to the "HARICA Certification Practice Statement/ Certification Policy" or a username/password provided during initial registration.

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

HARICA central RA always verifies device ownership. For SSL/TLS certificates used for domains belonging to Academic/Research institutions, a verification e-mail is sent to an institution's network operations center designated administrator 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 created in a SSCD).

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 according to which the subscriber'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 subscriber with the institution is certified.

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

3.2.6 Criteria for interoperability

HARICA may issue cross-certificates in order to assist ROOT roll-over operations and only for CAs under direct control of HARICA administration. All cross-certificates that identify HARICA as the subject shall be disclosed.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication for routine re-key

The user can request the issuance of a Re-key/Certificate fifteen (15) days before the expiration of the existing valid certificate, following the described procedures in section 3.2.

3.3.2 Identification and authentication for re-key after revocation

The user can request the issuance of a Re-key after the revocation of the initial certificate, following the described procedures in section 3.2.

3.4 Identification and authentication for revocation requests

As stated in section 3.2.3. Moreover, the CA and the subscriber agree to a secret revocation code during the retrieval of the certificate, which is necessary for the revocation of the subscriber's certificate by the actual subscriber.
Governmental regulatory authorities are authenticated via secure callback to their official telephone numbers or official e-mail addresses.

3.4.1 Issuing Authority

The Issuing RA/CA can 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 user'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 Subscriber

The subscriber can request a certificate revocation through the appropriate web interface, using the revocation secret code. Alternatively, a certificate revocation can be asked by the subscriber making a call to the appropriate Certification Authority therefore his identity MUST be verified using pre-existing information.

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 only by applicants as described in section 1.3.3.

4.1.2 Enrollment process and responsibilities

Subscribers may submit the application for the issuance of a certificate through the web page of the Registration Authority, http://www.harica.gr/, or through the Registration Authority of her/his own institution. 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 applications is based on what is outlined in section 3.2. All certificate applications are checked for validity.

4.2.2 Approval or rejection of certificate applications

After all identity and attribute checks of the applicant, 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. Otherwise the application is 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)

HARICA does not currently review CAA records as defined in RFC 6844.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate issuance

The certificates are published after the secure transmission of applications from the Registration Authority to the Certification Authority and after the successful verification of the contents of the certificate.

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 in order for the Root CA to perform a certificate signing operation.

4.3.2 Notification to subscribers by the CA regarding issuance of certificate

The Certification Authority informs the subscriber about the success or rejection of the publication of certificate via e-mail. In the same e-mail message, provided that the application is accepted, a unique URI is sent to the subscriber who MUST accept the terms and services of HARICA PKI before accepting and receiving the issued certificate.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The HARICA PKI subscribers MUST accept (retrieve and install through a secure webpage) the new certificate within **thirty (30) days**, otherwise the certificate is revoked and the subscriber must repeat the application process. The subscribers MUST declare on the secure webpage that they have checked all certificate elements and that they are correct, in order to retrieve their certificate. Finally, they accept the terms of use as they are described in this CP/CPS and then receive the certificate.

4.4.2 Publication of the certificate by the CA

All CAs publish the certificates only after they have been retrieved by the owners according to 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 9.16.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The HARICA PKI subscribers are allowed to use their private keys and certificates for the usages stated in section 6.1.7.

4.5.2 Relying party public key and certificate usage

Relying parties can use the HARICA PKI subscribers' public keys and certificates following what was stated in 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 the certificate is almost expired. Some certificates may be renewed using the same key pair provided that 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 renewal request is submitted by the subscriber wishing renewal through a secure web page after authentication. It is recommended that the beneficiary subscribers receive an e-mail message from the Registration Authority **fifteen (15) days** before the expiry date of their certificate and are informed for its imminent expiry. The subscribers make a certificate renewal request via a secure web page, after proper authentication.

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 user attributes, such as the certified name or email address, have changed, the procedures used for a new certificate application take place.
- For the rest of the permitted time period a new certificate is issued using the initial certificate request which is stored in the Certificate Authority.

For instance, a user 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 user certificates and **three (3) years** for server certificates.

4.6.4 Notification of new certificate issuance to subscriber

The same new certificate issuance procedure is followed, as stated in section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

The user/subscriber should receive the renewed certificate following the same procedure of acceptance and receipt of a new certificate, as stated in section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

The new certificate is published according the procedures stated in section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

No action is taken for the notification of other entities other than what is stated in section 9.16.

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. .

4.7.2 Who may request certification of a new public key

The beneficiary subscribers contact the CA in order to revoke their previous certificate. The subscribers afterwards make a certificate re-key request via a secure web page after proper authentication.

4.7.3 Processing certificate re-keying requests

The same re-key issuance procedure is followed, as stated in section 4.3.

4.7.4 Notification of new re-keyed certificate issuance to subscriber

The same re-key issuance procedure is followed, as stated in section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The user/subscriber MUST receive the certificate with the new key, following the same acceptance procedure, as described in section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

The certificate with the new key is published, according to the repository procedures, as stated in section 4.4.2.

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

No action is taken for the notification of other entities other than what is stated in section 9.16.

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 re-key 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 is revoked when it is not used anymore, 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. Moreover, the certificate is revoked when the subscriber 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 the certification policy. Finally, it is revoked if it contains erroneous information.

The loss of applicant's attribute or relationship, labor or other, with the institution or the specific unit in which she/he was originally a member (e.g. graduation, termination of employment), is a revocation reason as well.

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

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 chapter 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 material 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 (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name)
7. HARICA is made aware of a material change in the information contained in the Certificate
8. HARICA is made aware that the Certificate was not issued in accordance with this CP/CPS
9. HARICA determines that any of the information appearing in the Certificate is inaccurate or misleading
10. HARICA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
11. HARICA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate
12. Revocation is required by HARICA's Certificate Policy and/or Certification Practice Statement or
13. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. HARICA/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 of time).

4.9.1.2 Reasons for Revoking a Subordinate Certificate

HARICA shall revoke a Subordinate CA if it meets one or more of the reasons listed in section 4.9.1.1.

4.9.2 Who can request a revocation

The certificate can be revoked by the subscriber or by another entity that can prove the exposure or the misuse of the certificate according to the Certification Policy.

The secretariats or personnel services of the institution's units are obliged to make a revocation request for persons who lost their attribute under which they were certified.

In the special case of Qualified Certificates, the revocation of a certificate can be requested from governmental regulatory authorities and courts according to the local and European legislation.

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 according to 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

The Certification Authority must start the investigation of revocation requests within **one (1)** business day except from force majeure cases. Revocation requests that provide adequate supporting evidence, will be processed immediately.

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 intermediate Certification Authorities that intervene. The Revocation lists are always published in the Repository. A Certificate Revocation List shall include the status of a certificate at least until its expiration.

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.

4.9.7 CRL issuance frequency

The CRL must be updated and published:

- for end-user/device certificates, at least every **single (1) day**. The CRL will be in effect for a maximum time of **ten (10) days**.
- for CA certificates, 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 sub CA revocation, an updated Certificate Revocation List MUST be published within 24 hours from the revocation timestamp.

CRLs shall be stored in a protected environment in order 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)

An Online Certificate Status Protocol (OCSP) service operates under the HARICA PKI. The URL of this service is included in the issued certificates. The operation of an OCSP service is mandatory only for subordinate Certification Authorities that issue publicly trusted certificates.

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 of the HARICA PKI, they must also check every time the OCSP service of the HARICA PKI and inquire the status of all intermediate CAs. The URL of the OCSP service is included in all issued certificates. Operation of an OCSP service is mandatory only for subordinate Certification Authorities that issue publicly trusted 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 4.9.3.2.

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 for as long as HARICA is operational.

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.

4.10.3 Optional features

Not defined.

4.11 End of subscription

The subscription is terminated when a HARICA PKI certificate reaches the "validTo" date and expires. 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 located 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 into 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 equipment of the HARICA Public Key Infrastructure, is in air-conditioned rooms with power supply protected by Uninterruptible Power Supply units (UPS) and backup power generators.

5.1.4 Water exposures

The equipment of HARICA is located on raised flooring and not exposed to a large extent to flooding danger.

5.1.5 Fire prevention and protection

The equipment of the HARICA PKI is subject to the Greek law on prevention and fire protection in public buildings.

5.1.6 Media storage

The backup keys of HARICA Certification Authorities stored on external storage media (e.g. CD-ROMs) or other removable media MUST be 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.

Backup of the entire Public Key Infrastructure of HARICA, is kept on tape or memory flash disks kept by qualified executives.

Both of the previously mentioned storage media are in different physical locations, outside of the central servers of HARICA, 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 in order to avoid object re-use.

5.1.7 Waste Disposal

Waste containing any confidential information, such as floppy disks, hard disks etc. are destroyed before being discarded.

5.1.8 Off-site backup

There are off-site backups of all servers of the HARICA PKI. The CA backup keys are always stored encrypted. The decryption information is only known to the authorized personnel of each CA. The private keys of the Certification Authorities operated by the HARICA PKI are stored in an HSM. A backup of the entire Public Key Infrastructure of HARICA (except from the CA private keys) is stored in a magnetic tape held by authorized personnel. No single member of the authorized personnel has the capability to access a backup key. Both of the previously mentioned storage media are in different physical locations, protected from exposure to water and fire.

5.2 Procedural controls

5.2.1 Trusted roles

The personnel assigned to operate the CAs is considered to be trusted and authorized to perform all the works of the Certification and Registration Authorities under well-defined procedures. The roles and job descriptions of all personnel are clearly identified. Based on the 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

All personnel having trusted roles must authenticate themselves to the CA or the RA before performing their duties.

5.2.4 Roles requiring separation of duties

Personnel assigned to CA security roles shall be separated from personnel assigned to other normal operations.

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. A sufficient number of 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 operating the CA or RA with access to cryptographic procedures, is trained and educated on issues of the Public Key Infrastructure of HARICA by PKI experts. For this purpose there is adequate documentation that describes all the operational procedures of the infrastructure. Personnel working within the HARICA PKI needs 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.

5.3.7 Independent contractors requirements working outside GUnet and involved with the HARICA PKI

In case HARICA PKI 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

The HARICA PKI systems record applications for certificates, the issued certificates and CRLs, issued CAs and the messages exchanged with the Registration Authority. Furthermore, in all HARICA PKI servers, other processes of the operating system and applications are recorded such as connections and disconnections of the administrators, 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 on a daily basis.

5.4.3 Retention period for audit log

The transactions-events files are kept for **two (2)** years in order 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 transactions file is allowed only for reading to certain applications of the CAs and RAs 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.

5.4.4.3 Protection against deletions in transactions file

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

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 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

The records file relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is kept for at least **thirty (30) years** for "Qualified Certificates" and **seven (7) years** for non-qualified certificates for SSL use, after any Certificate based on that documentation ceases to be valid in order to be available for any lawful control. This period may be modified depending on developments of the relevant legislation.

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 recreated according to the procedures in section 4.1.

HARICA will make sure that when subCAs reach their expiration lifetime, they will stop issuing new certificates and will be replaced with new subCAs. Previous subCAs 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 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 breaches of systems and subsystems. If an anomaly or a suspected violation is detected, the service is suspended and a thorough check of all systems takes place.

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 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 system is restored from backups where there is no suspicion of violation, new security checks take place to find potential security holes and then the service returns online. In case of CA key compromise, the procedures of section 5.7.3 are followed.

5.7.3 Entity 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 Certification Authority are notified, all subscriber certificates issued by the compromised Certification Authority are revoked, along with the certificate of the Certification Authority. If the private key of the Root Certification Authority is compromised, each subCA MUST stop the service, notify all subscribers of all subordinate Certification

Authorities, proceed with the revocation of all certificates, issue a final CRL and then notify the relevant security contacts. 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

The HARICA PKI has the ability to operate continuously using backups of all systems/subsystems in a location outside the main premises of the HARICA servers according to 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 CA subscribers to switch to another Trust Service Provider. When the termination time is reached, each CA will revoke all issued certificates, update the relevant CRL and revoke its own 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 CA 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 according to this CP/CPS.

In either case, the files of the CA and RA relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is kept for **thirty (30) years** after any Certificate based on that documentation ceases to be valid in order to be available for any lawful control. This period may be modified depending on the relevant legislation.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The keys of the subscribers are generated by hardware and software at the candidate subscribers' 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 in order for the private keys to be under the possession of the recipient subscribers only.

Especially, in case a subscriber 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 usage of a crypto-token hardware device as defined in section 6.2.1.

The keys of the CAs are generated in a secure environment, either by special software and installed in cryptographic devices (Hardware Security Modules or HSMs),

or directly in an HSM. These cryptographic devices MUST comply with the hardware standards defined in section 6.2.1.

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

For the issuance of a ROOT or subordinate CAs, a well-defined key generation ceremony takes place, witnessed by an authorized committee. Especially for the issuance of a ROOT Certification Authority or for a subordinate Authority which is not under the control of the operator of the ROOT 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 the candidate subscriber or another entity or from the CA on behalf of the subscribers is not allowed. The delivery of the private key of the candidate subscriber to any third entity is not allowed.

If a Certification Authority allows the creation of private keys on behalf of another entity, the following or stricter procedure must take place:

- If the CA has enough information to confirm the validity of the identity of the user in advance, it has the ability to generate a key pair and a certificate for this user.
- The verification of the authenticity of this certificate is implemented when owners receive the credentials (certificate and keys) from the RA. This model is called "collective".
- The CA 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 the CA or any of its designated RAs 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), 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 subscriber 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 Vendors through appropriate Root CA Programs (for example Microsoft, Apple, Mozilla). HARICA subCAs, are available for secure download via the HARICA certificate repository described in section 2.1. The ROOT Certificate can also be found in the European Union's Trusted List of Certification Service Providers via the National

Supervisory Authority (Hellenic Telecommunications & Post Commission). 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 algorithm.

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. The 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 Certificate Profiles).

6.2 Private key protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

All CA private keys to be stored in a secure Hardware Security Module in order to perform key signing operations, 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 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) (Class A certificates), the private key MUST be generated and stored in a SSCD and cannot be extracted in any form. SSCD devices MUST meet at least FIPS PUB 140-2 level 3 or equivalent EAL 4+ or higher in accordance to ISO/IEC 15408 specifications.

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. The backup copy of the private key must be encrypted and the procedures referenced at section 5.1.6 must be followed. Access to the backup copy is allowed only by authorized personnel.

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 Certification Authority 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 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 private keys MUST be stored in a secure Hardware Security Module in order to perform key signing operations. Subscriber private keys can also be generated on a hardware cryptographic module. In the special case of Qualified Certificates with Secure Signature Creation Device (SSCD) (Class A certificates), the private key MUST be generated on a SSCD 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 or not to use the private key. Finally, private keys used in devices-services may be permanently activated and not protected at all using a passphrase, as long as 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 as long as the particular application that uses the certificate, is active.

For the key that relates to the ROOT CA, the key remains “active” only for the time required to perform cryptographic operations e.g. subCA key 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 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.

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 (20)** years for the Central CA, **ten (10)** years for a Subordinate CA, **five (5) years** for user certificates and **three (3) years** for server certificates. 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 the HARICA PKI 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 of 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

Not defined.

6.7 Network security controls

The connection of CAs 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

All time-stamping services -including logging operations- at HARICA PKI (either at the RA or the CA operations) MUST be synchronized via NTP (Network Time Protocol).

7 Certificate, CRL and OCSP Profiles

7.1 Certificate profile

A certificate profile according to RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile” is used.

7.1.1 Basic Certificate Contents

7.1.1.1 Version number

The version number of the certificates is 2, which corresponds to X.509v3 certificates.

7.1.1.2 Serial number

Unique system generated number assigned to each certificate. No duplicate serial numbers are allowed under the same CA.

7.1.1.3 Signature Algorithm

The algorithm used to sign the certificate. Limitations are described in section 7.1.3.

7.1.1.4 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.

7.1.1.5 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. HARICA limits country certificates to GR

The issuer DN must be unique in the HARICA PKI.

7.1.1.6 Valid From

The date on which the Certificate validity period begins (Format: DD/MM/YYYY HH:MM A.M/P.M GMT).

7.1.1.7 Valid To

The date on which the Certificate validity period begins (Format: DD/MM/YYYY HH:MM A.M/P.M GMT).

7.1.1.8 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 certificates): The e-mail address of the subject
- Common Name (CN) (Optional for SSL certificates): Subject Common Name. If present, for SSL certificates, this field MUST contain an FQDN that is one of the values contained in the Certificate's subjectAltName extension. For user certificates, this field MUST contain a user friendly representation of the person's name. Common names that also belong to the DNS namespace are forbidden.
- 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 (O): Subject Organization Name.
- Locality (L): Subject Locality.
- Country (C): Subject Country. HARICA limits country certificates to GR.
- 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.

7.1.2 Certificate extensions

Every issued certificate includes extensions as they are defined for X.509 v3 Certificates. Here is a list of extensions used in HARICA PKI. 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: 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 (smartcardlogon, clientAuth, serverAuth, emailProtection, codeSigning, Encrypting File System, TimeStamping, OCSP Signing, IP Sec, Document Signing). This list of values is not limited. Additionally, **it is forbidden** for subordinate CAs to issue certificates **with both** the serverAuth (1.3.6.1.5.5.7.3.1) and codeSigning (1.3.6.1.5.5.7.3.3) extended key usages.
- Qualified Certificate Statements (qcStatements): It provides one or more values that specify the attributes of the Qualified Certificate. The value id-etsi-qcs-QcCompliance which specifies that the certificate is Qualified following the Presidential Decree 150/2001 of the Hellenic Republic and Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures MUST always be present. Additionally, Class A certificates MUST include the value id-etsi-qcs-QcSSCD which specifies that the certificate was created at a hardware cryptographic device.

A list of the most common certificate profiles used by HARICA are listed in ANNEX B (HARICA 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 and subscriber 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

The name form is done according the rules of section 3.1.

7.1.5 Name constraints

HARICA constrains all of its subCAs according to RFC 5280. This extension is marked as “non-critical”.

Each subCA MUST be constrained to the domain name that the subCA signs for. For example, Aristotle University of Thessaloniki subCA will be limited to the “auth.gr” domain, using the name constraints extension.

Additionally, there are two sets of global subCAs, one that is restricted to the ".com" domain and one that is restricted to the rest of the domains (denies ".com" domain). Certificates will be issued from these subCAs only in case a subscriber requires a certificate on a domain that is not included in the name constraints of already issued subCAs. These CAs don't currently exist, but will be created upon first request of such a certificate.

Effective Dec 1st 2015, if a Subordinate CA Certificate includes the id-kp-serverAuth extended key usage and needs to be considered technically constrained and treated under the rules of section 8.1 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 sections 7.1.1 and 7.1.2.

If the Subordinate CA Certificate is 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.

Moreover, the 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.**26513.1.0.3.3**. According to each certificate class, the following recognized OIDs can be added in the certificatePolicies extension:

- 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: OID **0.4.0.2042.1.1**
- **NCP+** (Extended Normalized Certificate Policy) as described in ETSI TS 102 042: OID **0.4.0.2042.1.2**
- **DVCP** (Domain Validated Certificate Policy) as described in ETSI TS 102 042: OID **0.4.0.2042.1.6**
- **OVCP** (Organizational Validation Certificate Policy) as described in ETSI TS 102 042: OID **0.4.0.2042.1.7**

Subordinate CAs can use the reserved "AnyPolicy" OID **2.5.29.32.0** or in the case of externally operated CAs, the corresponding CP/CPS OID.

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 CP/CPS of HARICA PKI.

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 RFC 3280.

7.2.1.2 Signature Algorithm

The signature algorithm MUST be SHA1 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 will be issued in GMT. The requirements of section 4.9.7 apply.

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 Certification Authorities.

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 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" and*
- *the Precedential Decree 150/2001*.

HARICA PKI 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 as a result of deficiency

If a CA is shown to be non-conformant in any way to the specifications of ETSI TS 101 456 and ETSI TS 102 042, 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. 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 of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

During the period in which a Technically Constrained Subordinate CA issues Certificates, HARICA which signed the Subordinate CA 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 PKI cannot 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 and are explicitly and contractually bound to do so. HARICA staff and operators are trained on how to use and handle confidential information according to section 5.3.

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 generally not disclosed unless it is required by law or included in the certificate public information (for example the *subject* field of the certificate).

9.4.3 Information not deemed private

Information included in the issued digital certificates is not considered private.

9.4.4 Responsibility to protect private information

All private and personal information handled and processed by HARICA PKI is in accordance to the Greek legislation concerning personal data protection and the European Data Protection Directive. There are specific technical 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 Administration 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 PKI 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. All 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 Trusted 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.
- ✓ Immediately 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 this CP/CPS.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with this CP/CPS and for all liabilities and indemnification obligations of the Subordinate CA under this CP/CPS, as if the Root CA were the Subordinate CA issuing the Certificates.

9.6.1.1 Responsibilities of externally-operated Certification Authorities

Each externally-operated Certification Authority approved by HARICA PKI 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 immediately 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 an official audit certificate according to the latest versions of ETSI TS 101 456, ETSI TS 102 042 (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 for subscriber registration.

- ✓ 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 subscriber. 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 an official audit certificate according to the latest versions of ETSI TS 101 456, ETSI TS 102 042 (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 or Terms of Use 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, either:

1. The Applicant's agreement to the Subscriber Agreement with HARICA, or
2. The Applicant's agreement to the Terms of Use agreement.

The Subscriber or Terms of Use Agreement contain the following obligations and warranties:

- ✓ HARICA PKI subscribers are obligated 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.
- ✓ 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.
- ✓ 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.
- ✓ **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.

9.6.4 Relying Party Representations and Warranties

- ✓ 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.

- ✓ 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.

9.6.5 Representations and Warranties of Other Participants

Not defined

9.7 Disclaimers of warranties

Not defined

9.8 Limitations of liability

HARICA PKI cannot be held liable for any problems or damages that may arise from its services or from wrongful, negligent or improper use of the issued certificates. HARICA does not undertake any financial, civil or other responsibilities. 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 its operators.

9.9 Indemnities

HARICA PKI cannot be held liable and does not undertake any financial, civil or other responsibilities unless there is evidence of fraudulent intent or serious negligence by its operators. HARICA PKI cannot be used for transactions that are not included in the first paragraph of section 1.4.1. See also prohibited certificate uses as described in section 1.4.2. Therefore, HARICA PKI is exempt from any liability or damage that is not directly linked with the certification services for the already mentioned purposes.

9.10 Term and termination

This CP/CPS is valid and effective for as long as HARICA PKI is operational. When a subordinate Certification Authority or Registration Authority decides to terminate their services and withdraw from HARICA PKI, it is obliged to officially inform the Administration of HARICA. Similar correspondence is essential when an Organization wishes to participate and become a member of HARICA PKI.

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 PKI 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

Differences or disputes that result from the interpretation of the Certificate Policy/Certification Practice Statement and the operation of the Certification Authority will be solved according to the Academic deontology and the Greek Law.

In the case of disputes it is Greek courts that are competent and the venue is Athens Greece.

9.14 Governing law

HARICA is mainly focused on serving the Hellenic Academic and Research Community. The operation of the HARICA PKI as well as the interpretation of the CP/CPS adheres to the Greek Legislation and is subject to the Academic ethics. Particularly as far as the Presidential Decree 150/2001 «Adaptation to directive 99/93/EE of European Parliament and Council with regard to the Community frame for electronic signatures» is concerned, the issued personal certificates **ARE** considered "Qualified Certificates". HARICA PKI is listed in the Trusted Certification Authorities Registry of the Hellenic Telecommunications & Post Commission.

9.15 Compliance with applicable law

HARICA PKI is completely abided by the Greek Legislation.

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 Certificate Profiles)

Friendly Name	Policy IDs	Key Usages	Other Extensions
HARICA Subordinate Certification Authority Certificate	**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	**1.3.6.1.4.1.26513.1.0.3.3** **0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature** EKU: **OCSP Signing**	**OCSP No Check**
User Certificate	**1.3.6.1.4.1.26513.1.0.3.3** **0.4.0.2042.1.1 (NCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, Email Protection,** Encrypting File System (optional)	None
Qualified User Certificate	**1.3.6.1.4.1.26513.1.0.3.3** **0.4.0.1456.1.2 (QCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, Email Protection,** Encrypting File System (optional)	**QcStatements: id-etsi-qcs-QcCompliance**
Qualified User Certificate in Secure Signature Creation Device	**1.3.6.1.4.1.26513.1.0.3.3** **0.4.0.1456.1.1 (QCP+)**	KU: **Non Repudiation, Digital Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, Email Protection,** Smart Card Logon (optional)	**QcStatements: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD** SmartcardUser (optional)
User Certificate with Code	**1.3.6.1.4.1.26513.1.0.3.3**	KU: **Non Repudiation, Digital**	None

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

Signing	**0.4.0.2042.1.1 (NCP)**	**Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, Email Protection, Code Signing, Lifetime Signing,** Encrypting File System (optional)	
Qualified User Certificate with Code Signing	**1.3.6.1.4.1.26513.1.0.3.3** **0.4.0.1456.1.2 (QCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, Email Protection, Code Signing, Lifetime Signing,** Encrypting File System (optional)	**QcStatements: id-etsi-qcs-QcCompliance**
Qualified User Certificate in Secure Signature Creation Device with Code Signing	**1.3.6.1.4.1.26513.1.0.3.3** **0.4.0.1456.1.1 (QCP+)**	KU: **Non Repudiation, Digital Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, Email Protection, Code Signing, Lifetime Signing,** Smart Card Logon (optional)	**QcStatements: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD** SmartcardUser (optional)
Device Certificate	**1.3.6.1.4.1.26513.1.0.3.3** **0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature, Key Encipherment**[1] EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None
Enhanced Device Certificate	**1.3.6.1.4.1.26513.1.0.3.3** **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