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 3.2 (June 5th 2015)

Document Manager: Dimitris Zacharopoulos

Working Group: Dimitris Zacharopoulos
                     Fotis Loukos
                     Apostolos Papagiannakis
                     Ioannis Feneris

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

1   Introduction

The Public Key Infrastructure (PKI) for the Hellenic Academic and Research Institutions is supported and operated by the Greek Universities Network GUNet as a service to its members – all the Universities and Technological Educational Institutions – for servicing the education and research in our country. 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 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, conducted by Deventum and QMSCERT. 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, conducted by Deventum and QMSCERT. 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, v1.2.5" http://www.cabforum.org.

The globally unique Identification Number (OID) of this document is: 1.3.6.1.4.1.**26513.1.0.3.2** where:

1.3.6.1.4.1.**26513**	Identification Number (OID) of HARICA, registered to IANA (www.iana.org)
1	Certification Services Provision
0	Certification Practice Statement
3.2	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 HARICA-ROOT-CA certificates is twenty (20) 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 academic and research institutions 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 ten (10) years. The subordinate CAs that come initially into operation, certify entities that belong to HARICA (HARICA-Administration-CA). They issue

certificates for users and servers/devices of HARICA, but not for entities of other institutions. In case HARICA receives requests for entities of other Institutions, the relevant subordinate Central Certification Authorities will be created for each Institution. The creation of more than one subordinate CA is possible, e.g. the creation of the CAs (<Institution>-SUBSCRIBERS-CA and <Institution>-SERVERS-CA), that will issue the requested certificates but they will be signed by the Central CA of the Institution. Some CAs may be operated by the Institution itself, 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 in order to assist ROOT roll-over operations and only for CAs under direct control of HARICA administration. All cross-certificates that identify the CA as the subject shall be disclosed.

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 entities who request and successfully acquire a digital certificate signed by HARICA or any subordinate CA. Subscribers can be persons or devices that have a relationship with organizations within the Hellenic academic, research and educational community.

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 of an Institution, provided that the relevant procedure is described in the CP/CPS of the corresponding subordinate CA 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 the CA.
- √ 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

The certificates can be used by the members of the wider academic and research community and other parties as described in paragraph 1.3.

1.4.1 Appropriate certificate uses

The certificates can be used only for academic, administrative and research purposes, 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@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@harica.gr
Dimitris Zacharopoulos [d.zacharopoulos@auth.gr]
Tel: 2310 998483
Fax: 2310 999100

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

Spiros Bolis [sbol@noc.uoa.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@harica.gr

Dimitris Zacharopoulos [jimmy@it.auth.gr]
Tel: 2310 998483
Fax: 2310 999100

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

Spiros Bolis [sbol@noc.uoa.gr]
Tel: 210 7275611
Fax: 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. **Error! Hyperlink reference not valid.** All amendements 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

Long Term	Short term
Object Identifier	OID
Registration Authority	RA
Policy Certification Authority	PCA
Certification Authority	CA
Certification Practice Statement	CPS
Distinguished Name	DN
Domain Validation Cert. Policy	DVCP
Organizational Validation Cert. Policy	OVCP
Qualified Certificate	QCP

Qualified Certificate with SSCD	QCP+SSCD or QCP+
Trusted Third Party	TTP
Hierarchic Certification Structure	HCS
CommonName	CN
Certificate Revocation List	CRL
Certification Trust List	CTL
OrganizationName	O
Organizational Unit	OU
CountryName	C
Certification Policy	CP
Public Key Infrastructure	PKI
Policy Management Committee	PMC
Online Certificate Status Protocol	OCSP
Public-Key Cryptography Standards	PKCS
Secure Signature Creation Device	SSCD
Secure Socket Layer	SSL
Uniform Resource Identifier	URI

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 http://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).

The CA performs all the necessary actions for the uninterrupted - as possible - availability of its repository.

The HARICA PKI repository address is http://www.pki.auth.gr/rep_dyn.

Moreover, the storage and search of certificates and CRLs is possible using the directory service of HARICA or that of the participating institutions.

2.3 Frequency of publication

The CRL is updated according to the paragraph 4.9.7.

The certificates issued by the CA are being published immediately after their retrieval from the subscriber.

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

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 Type of Names

All information included in the certificates must be verified/validated at the time of issuance.

3.1.1.1   User certificates

The user certificates must include the full name of the user, his electronic address (according to rfc822), the name of institution she/he belongs to, and the abbreviation of her/his country.

Optionally, additional fields may be included, such as the organizational unit the user belongs to and her/his location.

3.1.1.2   Devices/Services certificates

Certificates that are issued for appliances (server, router or any other network device) must include the complete distinguished name of the appliance according to the Domain Name System (FQDN DNS), the name of institution it belongs to, and the abbreviation of the country. The certification of IP addresses or hostnames instead of the FQDNs is not allowed.

Optionally, additional fields may be included, such as the organizational unit the device's location.

3.1.1.3   Code Signing certificates

Code Signing certificates are provided through user certificates described in section 3.1.1.1. The user, in addition to the general terms-and-conditions of simple user certificates, is committed (via an appropriate extra RA agreement) to provide complete, accurate and truthful information (eg, application name, information URL, application description, etc.) in the digitally signed code.

The digital signing of malicious code (malware) is expressly prohibited.

Failure by a Subscriber to comply may result in revocation of the code signing certificate.

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.

3.1.3 Anonymity or pseudonymity of subscribers

The HARICA PKI does not allow certificate issuance for anonymous users. The certificate issuance for pseudonyms eg "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/accreditation with information that proves that the actual person holds the corresponding pseudonym/role. Eg. for the "Supervisor" role, there must be a document proving that the applicant is entitled to this role.

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 institution in which it belongs to "O" or/and "OU", the country to "C" and optionally the locality in which it is found to "L". It is preferable to adapt to the naming conventions used by the national directory service (today hosted at ds.grnet.gr). The HARICA User Certificates must include the attribute "C=GR" in the Distinguished Name.

3.1.4.2 Device certificates

The name of the device certificate (FQDN DNS) must correspond to the "Subject Alternative Name – SAN" field, the name of institution the device belongs to the characteristic "O" and/or "OU", the country the device is located in to the characteristic «C» and optionally the locality is found to the characteristic "L". 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. Device Certificates must include the attribute "C=GR" in the Distinguished Name.

3.1.5 Uniqueness of names

The Distinguished Name of a subscriber bearing attributes of a specific institution must be unique for the particular CA that issues the certificate, while it is desirable to be unique in the entire hierarchy of certification of HARICA. The issuance of more certificates with the same DN is allowed only in case of different class or certificate usage.

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 Registration Authority must verify that the alleged subscriber really possesses the private key that corresponds to the public key of the about-to-be-issued certificate. This is achieved with the following process:

- The identity of the subscriber is authenticated.
- An application for certificate issuance is submitted. The application contains the public key of the subscriber and has been signed with the private key of subscriber
- The key matching is verified.

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 Institution, the name of which is included in the certificate. The subscriber must:

a) be registered in the official directory service of her/his Institution and her/his Institution must appear in this record, or
b) Possess an electronic mail address in the official mail service of the Institution and the administration of her/his Institution confirms its relationship with the subscriber.

3.2.3 Authentication of individual person identity

3.2.3.1 Entity applying for the issue of a 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 on the SSCD. Class B includes certificates whose private keys have been 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 (eg 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.

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 three methods for e-mail ownership and control verification:

- The first method uses 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.

- The second method uses an 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.

- The third method uses a 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.

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

The individual who is in charge of the operation of the device and its conformity to the Certification Policy should possess a certificate which was issued by a CA that conforms to the "HARICA Certification Practice Statement/ Certification Policy".

The subscriber submits the application for a device certificate on a web interface where she/he must be authenticated presenting her/his personal certificate. The issuance of a certificate for a device owned by an institution other than the institution of its administrator, is not allowed.

HARICA central RA uses the following methods for device ownership verification. First of all, issuance of an SSL/TLS certificate is only allowed for domains belonging to each institution. Secondly, in order for a user to apply for an SSL/TLS device certificate he must own a user certificate which proves his identity. Then 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. He also checks that the person who applied for the certificate is the rightful owner of the FQDN according to the institution's database of users / servers.

In addition to the abovementioned procedures, a subscriber that requests a device certificate can be authorized by Domain Name Registrant as described in Section 11.1.1 of the CA/B Forum BR. For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by:

- Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;
- Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;
- Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;
- 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;
- Relying upon a Domain Authorization Document;
- 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
- Using any other method of confirmation, provided that the CA 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.

3.2.4 Non verified subscriber information

The certificates that are issued do not include non-verified subscriber information.

3.2.5 Validation of subscriber status

The Registration Authorities determine procedures according to which the subscriber's status and his conventional 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.

3.2.6 Criteria for interoperability

Not defined.

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 chapter 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 section, following the described procedures in section 3.2.

3.4 Identification and authentication for revocation requests

As stated in paragraph 3.2.3. Moreover, the CA and the subscriber agree to a secret revocation code during the retrieval of the certificate.

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 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 authorities
- if during auditing procedures it is found to contain false or inaccurate information
- if there is a relevant court order and
- in any case according to the 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 the subscribers as described in paragraph 1.3.3.

4.1.2 Enrollment process and responsibilities

The certificate DN of an applicant must be according to section 3.1. The validation of a user identity must be performed according to section 3.

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.

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. The subscriber's identity and official relationship with the institution are also checked.

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 verification of the DN of the certificate. The DN of the certificate of the applicant must agree with the specifications outlined in section 3.1.

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 cancelled 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 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

A certificate is revoked when it is not used any more, 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.

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 govermental 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

Submission of 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 institution does not exist any more
is required.

After revocation, the subject of the certificate will be informed of the change of status and the certificate shall never be reinstated.

4.9.4 Revocation request grace period

The subscriber can make a revocation request anytime during the validity period of the certificate. Certificate revocations can take place if the CA which issued these certificates is still in operation.

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.

The subscriber and the person in charge of the CA security are notified in case of exposure of the private key during the certificate revocation.

The CA 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

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

Relying parties can use one of the following offered services or a combination of these in order to decide for the validity of some certificates.

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

The CA 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

After the end of validity of the HARICA PKI certificates, the revocation 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

The Root Certification Authority of HARICA is currently located at the IT Center of Aristotle University of Thessaloniki. Other subordinate Certification Authorities may be located inside and outside AUTH IT Center.

Equipment, information and software relating to the Certification Authority and Registration Authority functions 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. The connection of the Root CA to any telecommunications network is prohibited.

In case unauthorized personnel need to enter into the physical location of the CAs and the RAs, they must never be left without oversight by an authorized person.

5.1.3 Power and cooling

All equipment of the HARICA Public Key Infrastructure currently hosted at AUTH IT Center, 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 currently hosted at AUTH IT site is not exposed to a large extent to flooding danger.

5.1.5 Fire prevention and protection

The equipment of the HARICA PKI currently hosted at AUTH IT Center is subject to the Greek law on prevention and fire protection in public buildings.

5.1.6 Media storage

The private keys of the HARICA Certification Authorities stored on external storage media (eg. CD-Roms) or other removable media MUST be in encrypted form, with a passphrase that is distributed in parts only to authorized personnel. No single member of the authorized personnel has the full passphrase to decrypt a private 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 private key of each CA is always stored encrypted. The decryption passphrase 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 detachable storage media. A backup of the entire Public Key Infrastructure of HARICA is stored in a magnetic tape held by authorized personnel. No single member of the authorized personnel possesses the private key and the complete passphrase to decrypt the private key at the same time.

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.

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 must be 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

Not defined.

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

Furthermore, 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 and the RA and has access to cryptographic procedures, is trained and educated on issues of the Public Key Infrastructure of HARICA by technicians of GUnet. For this purpose there is adequate documentation that describes all the operational procedures of the infrastructure. Personnel working within the HARICA PKI needs to know all policy / procedures documents, and the Certificate Practice Statement and the Certification Policy of the HARICA PKI in particular.

5.3.4 Re-training frequency and requirements

Not defined.

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 in 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** 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 time stamping of the records files is not required.

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 keys of the final certificates must be canceled and recreated according to the procedures in section 4.1.

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 abnormality 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 infringement on private keys. In case of violation without loss of private keys, 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. In case of lost keys, the procedures of the next paragraph are followed.

5.7.3   Entity private key compromise procedures

In case of loss of private keys or compromise of the algorithms and parameters used to generate the private key and certificate, 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 loss of a subordinate Certification Authority, all subscribers of this 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 lost, each CA 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 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*

Upon its termination, each CA informs its subscribers, revokes all issued certificates, updates the relevant CRL and revokes its own certificate. Furthermore, it informs the security officers and announces the end of its operation.In any case, the local and European legislation on the termination of Certification Authorities is followed.

The files of the CA and RA relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is kept for at least **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 paragraph 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 paragraph 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 his 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. The RA verifies a) the correctness of the signature and b) that the applicant is in possession of the corresponding private key.

6.1.4 CA public key delivery to relying parties

CAs provide mechanisms for the secure digital delivery of all certificates. Each digital certificate contains the public key when it is requested by interested entities. Interested entities may send a request by email. The CA can also send a certificate via snail-mail in a magnetic media device, which contains the public key. All certificates of each CA are published through a secure web site, whose identity is certified by a different trusted third party.

A suitable time before the expiration of a CA public key, a new certificate signing key pair will be generated in order to avoid disruptions to the normal CA operations.

Each CA publishes its certificate at the certificate store describe in section 2.1.

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.

Depending on the certificate class, certificate fields include at least the following uses:

Personal user certificate class:

Basic usages: 'Digital Signature', 'Non-Repudiation', 'Data Encipherment', 'Key Encipherment'.

Extensions: 'Client Authentication', 'Secure Email', 'Encrypting File System'

Device certificate class:

Basic usages: 'Digital Signature', 'Key Encipherment'.

Extensions: 'Client Authentication', 'Server Authentication'

Certificates with additional special services class:

Extensions: 'IP Security User', 'Timestamping', 'Code Signing', 'OCSPSigning'

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 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 code of the private key of every CA is segmented using a method described in an internal HARICA PKI document.

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 paragraph 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 key that corresponds to user and device 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 eg. 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

The CA private keys are destroyed using the secure deletion function of the Hardware Security Module. This destruction does not affect all copies of the private key. Only the physical instance of the key stored in the HSM under consideration will be destroyed. Only a combination of authorized personnel can destroy the private key of a CA. Subscribers are responsible for the destruction of their private keys, if they desire to do so.

6.2.11 Cryptographic module rating

Not defined.

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)** digits.

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 shall 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
Not defined.

6.6.2 Security management controls
Not defined.

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 paragraph 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. Must be unique in the HARICA PKI
- Organizational Unit (OU) (Optional if there is Issuing CN): Issuing Certification Authority. Must be unique in the HARICA PKI
- Organization (O): Organization Name
- Country (C): Issuing Country. HARICA limits country certificates to GR

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:

- 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
- 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) (Optional): Subject Locality
- Email (E) (Optional for SSL certificates): The e-mail address of the subject
- 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, it takes values *digitalSignature* (authentication), *nonrepudiation* (signing but only used with *digitalSignature* bit), *keyEncipherment* (encryption).
- certificatePolicies: explained in paragraph 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 algorithm MUST be SHA1 or stronger. Use of MD5 is prohibited along with other hashing algorithms that have been compromised. 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 CAs according to RFC 5280. This extension is marked as "non-critical".

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

Especially for the ".org" domain, in case an institution requires a server certificate for a particular educational or research activity (no user certificates will be allowed for this subCA), they will request it from a single subCA, limited only to ".org". This CA doesn't currently exist, but will be created upon first request of such a certificate.

Each subCA MUST be constrained to the Institution's 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.

7.1.6 Certificate policy object identifier

The OID (Object Identifier) of this certificate policy is 1.3.6.1.4.1.**26513.1.0.3.2**. 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.

7.2.1.5 Next Update
Date by which the next CRL will be issued. 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.

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 5 minutes to verify the freshness of the signed response. The hash algorithm used for the issuer name and key is SHA1.

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 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*. An external CP/CPS compliance audit is required on a yearly basis.

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).

A compliance audit may be conducted on demand by interested parties, provided there is appropriate permission by the institution which operates HARICA and as long as the interested parties cover the audit expenses.

If the 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.

9   Other Business and Legal Matters

9.1   Fees

No dues are paid for the provided services. All kinds of exploitation or subcontracting of provided services from their recipients is expressly prohibited.

9.1.1   Certificate issuance or renewal fees

No fees are charged

9.1.2   Certificate access fees

No fees are charged

9.1.3   Revocation or status information access fees

No fees are charged

9.1.4   Fees for other services

No fees are charged

9.1.5   Refund policy

No fees are charged

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

HARICA PKI does not handle commercial type of information.

9.4   Privacy of personal information

9.4.1   Privacy plan

Not defined.

9.4.2   Information treated as private

Private keys of the Certification Authorities, the source code and the private keys storage/operation procedures are considered classified and confidential information which are stored in the Certification and Registration Authorities. Information concerning the physical access and security of the premises where the Certification and Registration Authorities are installed and operated, is also considered classified.

It is likely that Registration Authorities undergo personal information processing during the identification procedure of the applicant.

9.4.3 Information not deemed private

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

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. The appropriate technical measures shall be taken 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 <u>non</u> 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 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.

9.4.8 Other information disclosure circumstances

Not defined.

9.5 Intellectual property rights

HARICA PKI does not hold any intellectual property rights on the issued certificates.

Anyone can copy parts of this CP/CPS with the condition that the original document is properly referenced.

9.6 Representations and warranties

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 is strictly used for Academic and Research activities and cannot be used for commercial, financial, legal or any other transactions that are not included in the first paragraph of section 1.4.1. 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.

9.11 Individual notices and communications with participants

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 Academic or Research Institution in Greece wishes to participate and become a member of HARICA PKI.

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 (eg revocation procedure).

9.12 Amendments

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

There will be prior notification to subscribers in case of major changes to the CP/CPS. 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 focused on serving the Hellenic Academic and Research Community. Each certificate issued, clearly states in the Certificate Policy Notice field that "*This certificate is subject to Greek laws and our CPS. This Certificate must only be used for administrative, academic, research or educational purposes*". 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 certificates that are published **ARE** considered as "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

9.16.1 Certification Authority Obligations

A Certification Authority is responsible for the issuance and the management of the certificates. Specifically HARICA certification authorities are bound to:
- ✓ Provide and maintain the infrastructure that is required for constitution of hierarchy of certification services for the Greek academic and research community, 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.

9.16.2 Responsibilities of subordinate Certification Authorities

Each subordinate Certification Authority approved by HARICA PKI is committed to:

✓ Grant certificates with validity period within the limits of the active employment (or other) relationship between the applicant and the institution, according to the applicant's affiliation (i.e student, employee, 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 institution -within the HARICA constituency- wants to run its own CA, 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).

9.16.3 Registration Authorities Obligations

Each Registration Authority manages the applications for subscriber registration.
✓ Each Registration Authority is responsible to receive certificate applications from subscribers. It validates the identity of the subscriber, confirms that the public key that is submitted belongs to the subscriber 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 user. The application includes all information identifying the subscriber, and the corresponding public key.
✓ Mass applications submission from a specific administrative department 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 institution -within the HARICA constituency- wants to run its own RA, 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).

9.16.4 Subscribers Obligations

- ✓ 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 certificates 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 (eg, application name, information URL, application description, etc.) in the signed code.

9.16.5 Relying party obligations

- ✓ 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.

9.16.6 Repository obligations

Each Certification Authority (root or intermediate) is obligated to operate and maintain a publicly accessible data repository containing:
- ✓ the certification authority certificate
- ✓ the Certificate Policy/Certification Practice Statement
- ✓ the HARICA Memorandum of Understanding
- ✓ the issued and retrieved certificates
- ✓ the Certificate Revocation Lists

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 ===

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	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature** EKU: **OCSP Signing, OCSP No Check**	**OCSP No Check**
User Certificate	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.1 (NCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection,** Encrypting File System (optional)	None
Qualified User Certificate	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.1456.1.2 (QCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection,** Encrypting File System (optional)	**QcStatements: id-etsi-qcs-QcCompliance**
Qualified User Certificate in Secure Signature Creation Device	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.1456.1.1 (QCP+)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** 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 Signing	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.1 (NCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment**	None

		EKU: **TLS Web Client Authentication, Email Protection, Code Signing, Lifetime Signing,** Encrypting File System (optional)	
Qualified User Certificate with Code Signing	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.1456.1.2 (QCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** 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	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.1456.1.1 (QCP+)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** 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	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	None
Enhanced Device Certificate	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, TLS Web Server Authentication, IPSec End System, IPSec Tunnel, IPSec User**	None