Memorandum of Understanding for the creation and support of HARICA

Hellenic Academic and Research Institutions Certification Authority

All institutions that sign the current MoU declare their common support for the creation and support of the **H**ellenic **A**cademic & **R**esearch **I**nstitutions **C**ertification **A**uthority (referred to as HARICA) and their mutual understanding and acceptance of the following terms.

1 HARICA as a common Trust Authority

Public Key Infrastructure (PKI) in general, is a combination of software, cryptographic technology, operations and services that produces an infrastructure for trust and security in network communications. Such an infrastructure will offer secure and confidential communications based on digital certificates used by authorized users and certified network resources.

The goal of this MoU is the consolidation of Public Key Infrastructures across different institutions into a single PKI named HARICA, which was originally hosted by the Greek Research and Technology Network (GRnet) and is now hosted and funded by the Greek Universities Network (GUnet). This Certification Authority will be the single Trust point (trust anchor) for the Hellenic Academic and Research community.

The implementation of this trust model is based on a hierarchical scheme with HARICA as a Root Certification Authority (ROOTCA).

The basic operational principles and requirements for joining-leaving HARICA PKI and trust scheme are described in the following paragraphs.

2 Joining the Trust Scheme

2.1 Operational requirements

For the creation of the trust relationship (to join the hierarchy) the following is required on behalf of HARICA:

- The Institution affirms that the subject identification procedures that will lead in certificate issuance will be reliable and according to the latest Certification Policy/Certificate Practice Statement (CP/CPS) of HARICA. These procedures will be adjusted according to the nature of the subject. The Institution will be held accountable for possible failures to maintain these procedures.
- All distinguished names used to define subjects must be distinct, clear and recognizable in the entire Hellenic academic and research community.
- The Institution provides proof of domain ownership. The methods of domain ownership verification are described in the CP/CPS document. There must be technical means at the RA and CA level to ensure that the issued certificates are limited to the domains that each institution has provided proof of ownership.

- The Institution agrees and complies with the HARICA Certification Policy/Certificate Practice Statement (CP/CPS) and signs this Memorandum of Understanding.
- HARICA MoU changes only by a unanimous decision of the participating Institutions, unless there are minor changes due to typo or grammatical errors. Its CP/CPS changes after approval by the designated Policy Management Committee (PMC).

2.2 Registration to the Trust Scheme

The organization responsible for operating HARICA and validating the conformance of new Institutions to this document is:
GUNET S.A.
Greek University Network GUnet
University of Athens – Network Operations Center
University of Athens Campus, Ilisia
157 84, Athens
Tel: +30-210 7275611
Fax: +30-210 7275601
ca-admin@harica.gr
Spiros Bolis [sbol@noc.uoa.gr]
Dimitris Zacharopoulos [d.zacharopoulos@auth.gr]
John Salmatzidis [jsal@it.auth.gr]

3 Operations within the Trust Scheme

Institutions that sign this MoU (including others that will sign in the future) are obligated to issue Certificates and Certification Authorities exclusively for subjects belonging to the same legal entity and constituency. Exceptions may be accepted, as long as there is unanimous decision of HARICA members.

4 Removal from the Trust Scheme

An institution may be removed from the trust scheme with the following ways:
a) The Institution decides to withdraw from the trust scheme.
b) The decision of the three fifths (3/5) of HARICA members, after the suggestion of HARICA operators due to non compliance with the terms of the current document and/or the policies and practices of HARICA CP/CPS. This will lead to the revocation of the Institutions subCA.
The removal from the trust scheme is performed with the following steps:

- The Institution sends a removal letter to HARICA via secure methods, signed by an authorized representative.
- HARICA validates the authenticity of the application and revokes the Certification Authority.
- HARICA creates and publishes the updated CRL.

5 Obligations of HARICA

HARICA Root is responsible for the issuance and maintenance of subordinate Certification Authorities. HARICA is specifically committed to:

- Install, maintain and secure the necessary infrastructure for the Root Certification Authority of the Hellenic Academic and Research Community.

- Accept or decline applications of institutions to join the HARICA trust scheme according to the terms, services and obligations defined in the current document.
- Administer a publically accessed repository of issued certificates and certificate revocation lists. This information must be published via a publically used protocol such as HTTP or LDAP. The publication of PKCS#7 files including the entire certificate chain of trust for each certificate is also desired.
- Revoke certificates when specific reasons apply or when a member decides to withdraw from the trust scheme as it is described in section 4.
- Treat all personal information provided by participating parties of HARICA as confidential.
- Immediately inform all technical staff in the event of exposure, loss, disclosure, modification or unauthorized usage of the HARICA ROOT CA private key.

Finally, the collaborating Institutions agree for team effort for the broad dissemination of Public Key in the Hellenic Academic and Research Community.

Agreed and signed by the following:

	Fullname/Title:
Technical Institution Representative for HARICA PKI	
Legal representative on behalf of the Institution:	
	Signed/sealed/dated
On behalf of HARICA:	**Prof. Lazaros Merakos** **Chairman of GUnet Management Committee**
	Signed/sealed/dated