

Greek Universities
Network (GUnet)



Hellenic Academic and Research Institutions

Public Key Infrastructure

Hellenic Academic and Research Institutions Certification
Authority (HARICA)

PKI Subscriber Agreement and Terms of Use

Version 1.0 (May 18th 2017)

Table of Contents

1	NOTICE	2
2	INTRODUCTION	2
2.1	DEFINITIONS AND ACRONYMS	2
2.1.1	<i>Definitions</i>	<i>2</i>
2.1.2	<i>Acronyms</i>	<i>7</i>
3	REPRESENTATIONS AND WARRANTIES	8
3.1	SUBSCRIBER REPRESENTATIONS AND WARRANTIES	8
3.2	RELYING PARTY REPRESENTATIONS AND WARRANTIES	9
3.2.1	<i>Information treated as private</i>	<i>10</i>
3.2.2	<i>Information not deemed private</i>	<i>10</i>
3.2.3	<i>Information disclosure to law enforcement and judicial agencies</i>	<i>10</i>
4	LIMITATIONS OF LIABILITY	10
5	INDEMNIFICATION	11
6	OTHER PROVISIONS	11
6.1	TERM AND TERMINATION	11
6.2	NOTIFICATION MECHANISM AND PERIOD	12
6.3	MODIFICATIONS TO SUBSCRIBER AGREEMENT	12
6.4	FORCE MAJEURE	12
6.5	DISPUTE RESOLUTION PROVISIONS	12
6.6	GOVERNING LAW – JURISDICTION	13
6.7	ENTIRE AGREEMENT	13

Version control

Version	Date	Comment
1.0	May 2017	<ul style="list-style-type: none">Subscriber Agreement and Terms of Use

1 NOTICE

PLEASE READ THIS CERTIFICATE SUBSCRIBER AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A HARICA DIGITAL CERTIFICATE.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT DO NOT APPLY FOR, ACCEPT, OR USE THE CERTIFICATE.

BY CLICKING “AGREE” WHEN YOU APPLY FOR OR BY ACCEPTING OR USING A CERTIFICATE, YOU AGREE TO BECOME A SUBSCRIBER AND BE BOUND BY THE TERMS OF USE CONTAINED IN THIS AGREEMENT AND THE APPLICABLE CP/CPS THAT ARE PUBLISHED IN THE REPOSITORY, WHICH ARE INCORPORATED BY REFERENCE INTO THIS AGREEMENT AND MADE INTEGRAL PART HEREOF.

2 Introduction

The Public Key Infrastructure (PKI) for the Hellenic Academic and Research Institutions is supported and operated by the Greek Universities Network GUnet (<http://www.gunet.gr>), a non-profit organization with members all the Universities and Technological Educational Institutions of Greece. This GUnet service, hereafter referred to as the Hellenic Academic and Research Institutions Certification Authority (HARICA), acts as a Trust Service Provider (TSP) also known as a “Certification Authority”, and as a “Qualified” Trust Service Provider (QTSP). In this Agreement, the terms “TSP” and “QTSP” are being used equally.

HARICA specifically acts as a “Root CA Operator”. The development and initial operation of the service began as part of the Virtual Network Operations Center (VNOC) project, funded by the National Research Network – GRNET (<http://www.grnet.gr>) and continues under the supervision and funding of GUnet. HARICA is operated and managed by Aristotle University of Thessaloniki’s IT Center. Organizations involved in this Public Key Infrastructure unconditionally accept this Certificate Practice Statement / Certificate Policy and co-sign a Memorandum of Understanding.

2.1 *Definitions and acronyms*

2.1.1 Definitions

In this Agreement, the following capitalized terms and expressions shall have the respective meaning ascribed to them below:

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

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

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: The natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant:

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

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

CA Certificate: A Certificate in which the basic constraints field has the CA attribute set to TRUE.

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

Certificate Data: The Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in HARICA's possession or control or to which HARICA has access.

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

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which HARICA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates.

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

Certificate Systems: The system used by a HARICA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Code Signing Certificate: A digital certificate that contains a code Signing ECU and is trusted in an Application Software Provider's root store to sign software objects

Coordinated Universal Time (UTC): The time scale based on the second as defined in Recommendation ITU-R TF.460-6.

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by HARICA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Key Compromise: A Private Key is considered to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

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

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

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

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

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

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

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

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

Qualified Certificate for electronic seal: A Certificate for Qualified Electronic Seal meeting the requirements of Annex III of Regulation (EU) No 910/2014

Qualified Certificate for electronic signature: A Certificate for Qualified Electronic Signatures meeting the requirements of Annex I of Regulation (EU) No 910/2014

Qualified Electronic Seal: An Advanced Electronic Seal that is created by a Qualified Electronic Seal Creation Device, and which is based on a Qualified Certificate for Electronic Seal, as specified in Regulation (EU) No 910/2014.

Qualified Electronic Signature: An Advanced Electronic Signature that is created by a Qualified Electronic Signature Creation Device, and which is based on a Qualified Certificate for electronic signatures, as specified in Regulation (EU) No 910/2014.

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

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

Registration Authority (RA): Any Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA Operator: The top-level Certification Authority (i.e. an organization) whose CA Certificate (or associated Public Key) is distributed by Application Software Suppliers as a trust anchor.

Root CA Certificate: A CA Certificate in which the Public Key has been digitally signed by its corresponding Private Key.

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

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

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

Subscriber Agreement: This agreement between HARICA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Terms of Use: The provisions contained in this Agreement regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the CP/CPS when the Applicant/Subscriber is an Affiliate of HARICA or IS HARICA.

Time-Stamp: Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

Time-Stamp Token (TST): A data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.

Time-Stamping Authority (TSA): The TSP providing time-stamping services using one or more time-stamping units.

Time-Stamping Unit (TSU): A set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

TSA Disclosure statement: A set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements.

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

2.1.2 Acronyms

Short Term	Explained Term
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DVCP	Domain Validation Certificates Policy
EKU	Extended Key Usage
EVCP	Extended Validation Certificates Policy
FIPS	United States Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
QCP	Qualified Certificate Policy
QCP+SSCD	Qualified Certificate Policy with Secure Signature Creation Device
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	On-line Certificate Status Protocol

OID	International Standards Organization's Object Identifier
OVCP	Organizational Validation Certificates Policy
PIN	Personal identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	IETF Working Group on PKI
PMC	Policy Management Committee
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSCD	Secure Signature Creation Device
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Socket Layer
subCA	Subordinate Certification Authority
TLD	Top Level Domain
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
TSP	Trust Service Provider
URL	Uniform Resource Locator
X.509	ITU-T standard for Certificates and authentication framework

3 Representations and warranties

3.1 Subscriber Representations and Warranties

The Subscriber represents and warrants the following:

- ✓ has read, accepts and shall comply with the Certificate Policy/Certification Practice Statement. Subscriber is obliged to use the certificates solely for the purposes described in the CP/CPS and the applicable law. HARICA Certificates cannot be used for money transactions (e.g. credit-card payments via e-shop) or for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger of life.
- ✓ shall create a key pair (private and public) using a reliable and secure system and shall take all necessary precautions to protect their private key from accidental destruction, loss or theft.
- ✓ After receiving the Certificate, the Subscriber shall review and verify that the information contained in the Certificate is accurate.
- ✓ shall promptly request the revocation of the Certificate when it is not used anymore, and cease using it when the data contained in it has changed or any information in the Certificate is or becomes incorrect or inaccurate, and if there is any actual or suspected misuse or when it is suspected that the private key has been compromised or lost.

- ✓ Especially in the case of Code Signing Certificates, the Subscriber is bound by the RA to provide complete, accurate and truthful information (e.g., application name, information URL, application description, etc.) in the signed code.
- ✓ **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to HARICA, both in the Certificate request and as otherwise requested by HARICA in connection with the issuance of the Certificate(s) to be supplied by HARICA.
- ✓ **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- ✓ **Responsiveness:** An obligation to respond to HARICA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- ✓ **Acknowledgment and Acceptance:** An acknowledgment and acceptance that HARICA is entitled to revoke the certificate immediately if the Subscriber were to violate the Terms of Use of this Agreement or if HARICA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

In the case of HARICA TSA Subscribers,

- ✓ must verify that the requested TST has been signed by a TSU private key that corresponds to a valid HARICA TSU Certificate and check for possible revocations.
- ✓ must use Time-Stamps from HARICA TSUs in combination with a valid signing (un-revoked) Certificate.

3.2 Relying Party Representations and Warranties

- ✓ HARICA Certificates cannot be used for money transactions (e.g. credit-card payments via e-shop) or for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger of life.
- ✓ Entities that trust the issued certificates are obligated to read and accept this Certificate Policy/Certification Practice Statement and to use the certificates only in ways that conform to this CP/CPS and the current legislation.
- ✓ Entities that trust the certificates must check the validity of the digital certificate signature and trust the parent Certification Authorities. Finally, they should periodically check the validity of the certificate against the relevant Certificate Revocation List of use the Online Certificate Status Protocol (OCSP) service for possible revocations.
- ✓ Entities that trust the certificates must check the Extended Key Usage X.509 Extension in the End-Entity Certificate and Issuing CA Certificate for the appropriate use of the certificates.
- ✓ Collect enough information to determine the extent to which they can rely on a digital certificate
- ✓ Bear full and sole responsibility for any decision to rely on a digital certificate
- ✓ Bear the full consequences, including legal liability, for any failure to observe their obligations and responsibilities as detailed in this CP/CPS.

- ✓ Entities that trust the Time-Stamps must verify that the TST has been signed by a TSU private key that corresponds to a valid HARICA TSU Certificate and check for possible revocations and that the private key used to sign the time-stamp has not been compromised until the time of the verification. If this verification occurs after the expiration date of the TSU Certificates, the provisions of Annex D of ETSI EN 319 421 provide guidance.
- ✓ Entities that trust the Time-Stamps must consider any limitations of the usage of the time-stamp indicated by the time-stamp policy and consider any other precautions prescribed in agreements or elsewhere.
- ✓ Entities that trust the Time-Stamps as “Qualified”, must use the designated EU “Trusted List” to establish whether the time-stamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified.

3.2.1 Information treated as private

Registration Authorities undergo personal information processing during the identification and validation procedure of the Applicant which is treated as private. Personal information is not disclosed unless it is required by law or included in the certificate public information (for example the *subject* field of the certificate) with Applicant’s consent. If the Applicant agrees to include personal information related to personal identification described in CP/CPS Section 7.1.4.7 (Social Security Number, Personal Identification, Tax Identification, Passport Number) in the Subscriber Certificate, then this information is not considered private.

3.2.2 Information not deemed private

Information included in the issued digital certificates is not considered private. If the Applicant, during the Certificate request process, requested personal information to be embedded in the issued Certificate, the Subscriber consents to HARICA’s disclosure of this information publicly by embedding the information in the issued Certificate. Subscriber Certificates are publicly disclosed at HARICA’s Repository, which implements restrictions to protect against enumeration attacks.

3.2.3 Information disclosure to law enforcement and judicial agencies

All non-classified information stored at the Certification and Registration Authorities is available to the law enforcement authorities, after their official written request. Classified and personal information can be disclosed to the judicial authority if there is an official court order according to the privacy and data protection applicable law. The process is carried out through the Management Committee of HARICA.

4 Limitations of liability

This Clause 4 applies to liability under contract (including under any indemnity or breach of warranty), in tort (including negligence), under statute or otherwise for non – compliant usage of the certificate(s) the associated private keys, the revocation status information or any other hardware or software provided, and any consequential, incidental,

special, or exemplary damages arising out of or related to this Agreement, including but not limited to, loss of data, loss of business and loss of profit.

To the extent permitted by applicable law HARICA cannot and shall not be held liable for any problems or damages that may arise from its services 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 Agreement and the 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. HARICA shall not be liable to the Subscriber for any loss suffered by the Subscriber due to use of a Certificate outside the normal and intended use.

Subject to this Clause 4 and to the provisions contained in the CP/CPS, HARICA's maximum aggregate liability under this Agreement sustained by the Subscribers is limited to a maximum of 1.000€ per Certificate for Qualified Signatures/Seals and a total maximum of claims of 1.000.000€, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The Liability limitations provided in this paragraph shall be the same irrespective to the number of Certificates for Qualified Signatures/Seals, transactions, or claims related to such Certificate. The limitations on Liability provided herein shall apply to the maximum extent allowed under the applicable Law of the applicable jurisdiction.

5 Indemnification

The Subscriber shall indemnify HARICA and its affiliates and their respective directors, officers, employees and agents (each an "Indemnified Person") against all liabilities, losses, expenses or costs (collectively "Losses") that, directly or indirectly are based on Subscriber's breach of this Agreement, information provided by the Subscriber or Subscriber's or its customers' infringement on the rights of a third party.

The indemnification obligations of the Subscriber are not HARICA's sole remedy for Subscriber's breach and are in addition to any other remedies HARICA may have against the Subscriber under this Agreement. The Subscriber's indemnification obligations survive the termination of this Agreement.

6 Other provisions

6.1 Term and Termination

Term. Unless otherwise terminated as allowed herein, this Agreement is effective upon Subscriber's acceptance and shall continue for as long as a Certificate issued under this Agreement is valid.

Termination. Either Party may terminate this Agreement for convenience by providing the other party twenty (20) business days' notice. HARICA may terminate this Agreement immediately without notice if

- (i) Subscriber materially breaches this Agreement
- (ii) HARICA revokes a Certificate as allowed herein and in the CP/CPS
- (iii) HARICA rejects Subscriber's Certificate application

- (iv) HARICA cannot satisfactorily validate Subscriber in accordance with the provisions of this Agreement and the CP/CPS, or if
- (v) Industry standards or changes in applicable legislation affect the validity of the Certificates requested by the Subscriber.

6.2 Notification mechanism and period

In case of major changes to the CP/CPS, Subscribers will be notified in advance to the effective dates. HARICA is obligated to publish (at its web site), previous versions of its CP/CPS in case of major document changes. The most recent CP/CPS is always published at the following URL: <http://www.harica.gr/documents/CPS.php>.

6.3 Modifications to Subscriber Agreement

HARICA may (i) revise the terms of this Agreement; and/or (ii) change part of the services provided herein at any time. Any such change shall be notified to the Subscriber by any convenient way and in any case, shall be binding and effective fourteen (14) days after publication of the changes in this Agreement and/or in the CP/CPS on HARICA'S web site <http://www.harica.gr>, or upon notification to the Subscriber by e-mail. If the Subscriber continuous to use its Certificate after the date on which the terms of this Agreement have changed, HARICA will treat such use by the Subscriber as acceptance of the updated terms. This Agreement may only be amended or modified by the HARICA PMC except as expressly specified herein.

6.4 Force Majeure

Neither party will be liable for failure to perform any obligation under this Agreement to the extent such failure is caused by a force majeure event (including acts of God, natural disasters, war, civil disturbance, action by governmental entity, strike and other causes beyond the party's reasonable control). The party affected by the force majeure event will provide notice to the other party within a reasonable time and will use reasonable efforts to resume performance as soon as practicable. Obligations not performed due to a force majeure event, will be performed as soon as reasonably possible when the force majeure event ceases.

6.5 Dispute resolution provisions

If a dispute or difference arises in connection with, or out of the interpretation of the Certificate Policy/Certification Practice Statement, the operations of the Certification Authority, and/or this Agreement, the Subscriber may address this dispute to the HARICA Policy Management Committee and shall attempt to resolve or settle such dispute in an amicable way before commencement of any legal proceedings. HARICA Policy Management Committee is responsible to investigate all matters concerning complaints and disputes about the provisioning of the trust services. See also CP/CPS section 3.1.6.

6.6 Governing law – Jurisdiction

This Agreement will be interpreted, construed and enforced in all respects in accordance with the applicable European and Greek legislation. All proceedings or legal action arising from this Agreement must be commenced in the courts of Athens Greece. Both parties agree to the exclusive venue and jurisdiction of Athens courts, Greece.

6.7 Entire Agreement

This Agreement and all documents referred to herein constitutes the entire agreement between the parties, superseding all other agreements that may exist with respect to the subject matter.