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 1.6 (Oct 17th 2022)

Table of Contents

Version control

Version	Date	Comment
1.0	May 2017	• Subscriber Agreement and Terms of Use
1.1	Feb 2018	• Update to include Applicant obligations for Intellectual Properties
1.2	Oct 2018	• Update to clarify information related to Personal Information. Related sections from CP/CPS were added.
1.3	Mar 2019	• Update to align with CP/CPS version 3.8
1.4	Oct 2019	• Update to align with CP/CPS version 3.9
1.5	Mar 2020	• Update to align with CP/CPS version 4.0
1.6	Oct 2022	• Update to align with CP/CPS version 4.6

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.

BY CLICKING "AGREE" WHEN YOU APPLY FOR OR BY ACCEPTING OR USING A CERTIFICATE, YOU ALSO AGREE THAT YOU HAVE READ, UNDERSTAND AND ACKNOWLEDGE THE DATA PRIVACY STATEMENT ISSUED BY HARICA/GUNET AVAILABLE AT https://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf.

2 Introduction

The Public Key Infrastructure (PKI) for the Hellenic Academic and Research Institutions is supported and operated by the **Greek Universities Network (GUnet)** (https://www.gunet.gr), a non-profit civil law company with members all the Universities of Greece, with VAT number **EL099028220**, General Commercial Registry number **160729401000** and Registration of Incorporation number **13392/28-9-2000** lawfully registered in the company's records of the Athens Court of First instance. This GUnet service, hereafter referred to as the Hellenic Academic and Research Institutions Certification Authority (HARICA), acts as a Trust Service Provider (TSP) also known as a "Certification Authority", and as a "Qualified" Trust Service Provider (QTSP). For the rest of this CP/CPS, the terms "TSP" and "QTSP" will be used equally.

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

2.1 Definitions and acronyms

The Definitions found in the CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

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, or any entity operating under the direct control of a Government Entity.

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

Applicant Representative: A natural person acting on behalf of the Applicant, in a legally binding manner, who is employed either by the Applicant or an agent duly authorized 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 HARICA 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 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 EKU 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 contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

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, as the subject of rights and obligations 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 that is issued by a qualified trust service provider and meets the requirements of Annex III of Regulation (EU) No 910/2014.

Qualified Certificate for electronic signature: A Certificate for Qualified Electronic Signatures that is issued by a qualified trust service provider and meets the requirements of Annex I of Regulation (EU) No 910/2014.

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

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

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

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

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.

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.

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes.

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
CT	Certificate Transparency
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
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
UTC	Coordinated Universal Time
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 HARICA's Certificate Policy/Certification Practice Statement. Subscriber is obliged to use the certificates solely for the purposes described in the CP/CPS Section 1.4.1 and the applicable law. HARICA Certificates cannot be used for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger of life.
- ✓ the Subscriber's request for certificate and issuance of the certificate itself is clear from any third-party intellectual property or proprietary rights, does not contain data which in any way interferes with or infringes upon the rights of any third party in any jurisdiction with respect to patents, trademarks, service marks, trade names, company names, "doing business as" (DBA) names and other trade rights, and does not present the data for any unlawful purpose whatsoever. Data covered by this representation and warranty includes but is not limited to any domain name, domain name space, Distinguished Name (DN), or Fully Qualified Domain Name (FQDN), and/or any trade name or DBA name, contained in any part of the certificate request.
- ✓ 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 certificate revocation when it is not used anymore or when the data contained has changed or when it is suspected that the private key has been compromised or lost. Failure to request revocation of the Certificate,

the Subscriber acknowledges and accepts that has no claim for liability, in case of mis-use of the private key or the Certificate, when it should have been revoked.

- ✓ For TLS Certificates, when the Subscriber requests revocation, the most appropriate revocation reason should be selected, as described in the CP/CPS section 4.9.1.1.
- ✓ **Accuracy of Information:** An obligation and warranty to always provide accurate and complete information 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.

In the case of HARICA Code Signing Subscribers, in addition to the above obligations and warranties:

- ✓ **Protection of Private Key:** Where the key is available outside a Signing Service, to maintain sole control of, keep confidential, and properly protect, at all times in accordance with CP/CPS section 6.2.7.4, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). HARICA SHALL provide the Subscriber with documentation on how to protect a Private Key. HARICA MAY provide this documentation as a white paper or as part of this Subscriber Agreement. The Subscriber SHALL represent that it will generate and operate any device storing private keys in a secure manner, as described in a document of code signing best practices, which HARICA SHALL provide to the Subscriber during the ordering process. HARICA SHALL obligate the Subscriber to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
- ✓ **Private Key Reuse:** To not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.
- ✓ **Use:** To use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

Depending on the type of Certificate issued and the corresponding certificate hierarchy, Subscribers and HARICA must comply with the **certificate revocation and suspension requirements** described in section 4.9 of the CP/CPS.

3.2 Relying Party Representations and Warranties

- ✓ HARICA Certificates cannot be used 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.

3.3 Privacy of personal information

3.3.1 Privacy plan

HARICA has implemented a Data Protection Policy and issued its Data Privacy Statement, available at https://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf in compliance with applicable laws relating to data protection and any equivalent legislation and EU Regulations.

3.3.2 Information treated as private

Registration Authorities undergo personal information processing during the identification and validation procedure of the Applicant which is treated as private. Personal information is not disclosed unless it is required by law or included in the certificate public information (for example the *subject* field of the certificate) with Applicant's consent. If the Applicant agrees to include personal information related to personal identification described in 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.

3.3.3 Information not deemed private

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

3.3.4 Responsibility to protect private information

All private and personal information handled and processed by HARICA, is in accordance with the Greek legislation concerning personal data protection. There are specific technical and organizational measures in place to prevent unauthorized and unlawful processing or accidental loss of private and personal information.

3.3.5 Notice and consent to use private information

Unless otherwise stated in this CP/CPS, the applicable Data Privacy Statement (available at https://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf) or by agreement, all private and personal information handled and processed by HARICA are not used without prior notice or consent, where applicable, of the data subject to whom it concerns, in accordance with applicable data protection laws and any equivalent legislation and EU Regulations.

3.3.6 Disclosure pursuant to judicial or administrative process

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 a properly constituted and enforceable instrument is issued, such an official court order, judgment or administrative action or demand, in accordance with general principles of law and applicable legislation.

The process is carried out through the Policy Management Committee of HARICA (see section 1.5 of CP/CPS). Private keys used to sign and issue digital certificates are never disclosed to any third parties, unless HARICA is obliged to such disclosure under applicable and enforceable law.

3.3.7 Other information disclosure circumstances

All non-classified and non-private information stored at the Certification and Registration Authorities is available for entity queries, upon request for reasons of legitimate interest.

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

This clause is subject to applicable data protection laws and EU Regulations.

3.3.7.1 Publicity

By accepting the Terms, Subscriber grants HARICA the right to use Subscriber's brand name and/or logo, to identify as a customer on HARICA's website or other marketing or advertising materials without any previous notice.

Subscribers may opt out by informing HARICA at support@harica.gr, within the first 30 days of their subscription

3.3.8 Intellectual property rights

HARICA owns the intellectual property rights for its PKI services. It does not hold any intellectual property rights on the keys of Subscriber's issued certificates.

Any reproduction, copying or outright reference of the CP/CPS is prohibited, without explicit reference to its original text.

Parts of the CA/B Forum Baseline Requirements, Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates, Mozilla and Microsoft Root Program Requirements are used in this document and the CP/CPS.

Subscribers shall not use HARICA's trademark without any previous notice and HARICA's written consent.

3.4 Audit logging procedures and Records Archival

3.4.1 Types of events recorded

HARICA Certificate Systems log all transactions related to certificate applications, issuance or revocations of certificates, issuance of CRLs, issuance or revocations of CA Certificates and all information exchanged with the Registration Authority. Furthermore, all HARICA PKI servers, log operating system processes, authentication attempts, HTTP connections to web servers, etc. All servers that record logs are synchronized via NTP (Network Time Protocol).

3.4.2 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. Multiple copies of audit logs are stored in different locations and protected by appropriate physical and logical access controls.

3.4.3 Audit log backup procedures

A backup of the transactions-events file is kept in different location in read-only mode, protected by appropriate physical and logical access controls.

3.4.4 Vulnerability assessments

HARICA performs an annual Risk Assessment that:

1. identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management processes;
2. assesses the likelihood and potential damage caused by these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management processes; and
3. assesses the adequacy of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Periodic Penetration Tests, at least annually, and quarterly Vulnerability Scans are conducted by a highly skilled security team with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

3.4.5 Types of records archived

All records of transactions referred to in section 3.4.1, and all documentation related to requests for issuance / revocation of digital certificates are confidentially archived.

3.4.6 Retention period for archive

Archived audit logs (as set forth in the CP/CPS section 5.5.1) SHALL be retained for a period of at least

- **Seven (7) years** for "Qualified Certificates for electronic signatures/seals",
- **Two (2) years** for SSL/TLS, Code Signing and non-qualified Client Certificates
- **one (1) year** for Time-Stamping Certificates

from their record creation timestamp, or as long as they are required to be retained per CP/CPS section 5.4.3, whichever is longer.

Additionally, HARICA and each delegated party SHALL retain, for at least two (2) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in the CP/CPS section 5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in CP/CPS section 5.5.1) after the later occurrence of:
    a. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
    b. the expiration of the Subscriber Certificates relying upon such records and documentation.

These retention periods shall be modified according to the relevant data protection laws.

4 Limitations of liability

This clause applies to liability under contract (including under any indemnity or breach of warranty), in tort (including negligence), under statue or otherwise for non – compliant usage of the certificate(s) the associated private keys, the revocation status information or any other hardware or software provided, and any consequential, incidental, special, or exemplary damages arising out of or related to HARICA's CP/CPS, including but not limited to, loss of data, loss of business and loss of profit. Except as set out in the next paragraph, and to the extent permitted by applicable law, HARICA cannot and shall not be held liable for any problems or damages that may arise from its services in case of wrongful, negligent or improper use of the issued certificates. HARICA does not undertake any financial, civil or other responsibilities for such cases. Using HARICA and its certification services requires that users unconditionally accept the terms and services and that HARICA is not liable and does not undertake any financial, civil or other responsibilities, except for cases where there is evidence of fraudulent intent or serious negligence by HARICA or its operators. HARICA shall not be liable to the Subscriber for any loss suffered by the Subscriber due to use of a Certificate outside the normal and intended use. Subscribers are obliged to request Certificate revocation for reasons stated in the CP/CPS section 9.6.3. Failure to request revocation of the Certificate, voids any liability claims if the private key or the Certificate is mis-used, when it should have been revoked with actions originating from the Subscriber.

If HARICA deviates significantly from the provisions set forth in the CP/CPS when issuing "**Certificates for Qualified electronic signatures**", "**Certificates for Qualified electronic seals**", "**Qualified Certificates for web site authentication**", "**Extended Validation Certificates for SSL or Code Signing**", certain liability provisions apply:

- HARICA is only liable for the correct verification of the application and the resultant contents of the Certificate (except for the "OU" field as stated in the CP/CPS section 9.6.2).
- HARICA shall not be liable if the Applicant/Subscriber supplied false or tampered validation evidence and information from this evidence was included in the Certificate. In this case, the Subscriber is liable for damage which HARICA and/or GUnet may suffer due to incorrect data being included in the Certificate or if the Subscriber uses such a Certificate in an incorrect way.

Except for the previous cases, HARICA's liability under the CP/CPS sustained by Subscribers or Relying Parties is limited to a maximum of **2.000€ per Certificate for Qualified Signatures/Seals, Qualified Certificates for website authentication, Extended Validation Certificates for SSL and Extended Validation Certificates for Code Signing** 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, transactions, or claims related to such Certificate. The limitations on Liability provided herein shall apply to the maximum extent allowed under the applicable Law of the applicable jurisdiction. This is covered via a Professional Liability/Errors and Omissions insurance, with policy limits of five

million Euros (5.000.000€) in coverage, including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining Certificates for Qualified Signatures/Seals, Qualified Certificates for web site authentication, Extended Validation Certificates for SSL and Extended Validation Certificates for Code Signing, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

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, any information, misrepresentation or breach of warranty or covenant provided by the Subscriber or Subscriber's or its customers' interference or infringement upon the rights of any third party and shall be responsible for defending all actions against an Indemnified Person.

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.

In case of a planned termination decision, HARICA will provide a timely notice to all Subscribers to switch to another Trust Service Provider. When the termination time is reached, each Subordinate CA Operator will revoke all issued certificates, update the relevant CRL and revoke its own certificate. This revocation process includes all TSU Certificates and its Issuing CA Certificate. Furthermore, it informs the appropriate authorities and announces the end of its operation. In any case, the local and European legislation on the termination of Certification Authorities is followed.

In case of a transfer of HARICA operations to another accredited TSP, a thorough migration plan will be created. All Subscribers will receive due notice of this transfer and decide whether they wish to switch to another TSP or not. During the transfer, all critical operations are expected to continue to function properly.

6.2 Notification mechanism and period

In case of material 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 material document changes. The most recent CP/CPS is always published at the following URL: https://repo.harica.gr/documents/CPS.

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 https://repo.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.

6.4 Resolution Process regarding disputes about naming property rights and the role of trademarks

The Subscriber represents and warrants, by submitting a certificate request that their request is clear from any third-party intellectual property or proprietary rights, does not contain data which in any way interferes with or infringes upon the rights of any third party in any jurisdiction with respect to patents, trademarks, service marks, trade names, company names, "doing business as" (DBA) names and other trade rights, and does not present the data for any unlawful purpose whatsoever. Data covered by this representation and warranty includes but is not limited to any domain name, domain name space, Distinguished Name (DN), or Fully Qualified Domain Name (FQDN), and/or any trade name or DBA name, contained in any part of the certificate request.

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.

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 Assignment

Relying Parties and Subscribers shall not assign any of their rights, interests or obligations hereunder (whether by operation of law or otherwise), without the prior written consent of HARICA. Any such attempted assignment shall be null and void. Subject to the foregoing, this Subscriber Agreement shall be binding upon and inure to the benefit of the parties hereto, their successors and permitted assignees.

6.8 Force Majeure

The occurrence of a Force Majeure event constituting a delay in the performance or fulfillment of any of the particular obligation on the part of HARICA hereunder shall not be used as a right of the Relying parties or Subscriber or any third party to make a claim for compensation against HARICA neither HARICA shall be liable for any default or delay caused directly or indirectly due to Force Majeure. Force Majeure means the exceptional events or circumstances to the extent that they are beyond HARICA's reasonable control. Conditions beyond HARICA's reasonable control include, but are not limited to natural disasters such as fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the Hellenic Republic, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of HARICA.

6.9 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.

6.10 Data Protection

The Subscriber acknowledges that HARICA/GUNET has provided the Subscriber with sufficient information with regard to Data Protection Policy implemented by HARICA and Subscriber's rights as data subject in this respect and that it has read, understand and acknowledges the DATA PRIVACY STATEMENT issued by HARICA/GUNET acting as "Data Controller", which is located at https://repo.harica.gr/documents/Data-Privacy-Statement-EN.pdf.

Furthermore, the Subscriber acknowledges that certain information provided at the time of application will be embedded in a digital certificate, and may be published in a directory of certificates. This information may also be used for revocation procedures and for the purpose of operating the certificate services.

The Subscriber understands that by providing this information when applying for a Certificate, it consents to HARICA's disclosure of this information for these purposes necessary for the performance of this Subscriber Agreement and the provision of the relevant trust services or products, and understands that it has the right to correct any related personal information.