Greek Universities Network (GUnet)

Hellenic Academic and Research Institutions

Public Key Infrastructure

Hellenic Academic and Research Institutions Certification Authority (HARICA)

PKI Disclosure Statement (PDS) for the Hellenic Academic and Research Institutions Certification Authority

Version 1.0 (May 18th 2017)

Table of Contents

Version control

Version	Date	Comment
1.0	May 2017	• Initial PDS to comply with ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 421

1 Introduction

The Public Key Infrastructure (PKI) for the Hellenic Academic and Research Institutions is supported and operated by the Greek Universities Network GUnet (http://www.gunet.gr), a non-profit organization with members all the Universities and Technological Educational Institutions of Greece. This GUnet service, hereafter referred to as the Hellenic Academic and Research Institutions Certification Authority (HARICA), acts as a 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.

This document is a PKI Disclosure Statement following the structure of ETSI EN 319 411-1 (Annex A). It is a supplemental instrument of disclosure and notice by HARICA to Subscribers and Relying Parties and does not replace or substitute the latest version of HARICA Certificate Policy and Certificattion Practice Statement (CP/CPS), published at https://www.harica.gr/documents/CPS.

2 TSP contact information

2.1 Policy Making Organization

HARICA CP/CPS and all subscriber/third-party agreements, security policy documents and procedural documents, are administered by HARICA Policy Management Committee (PMC), appointed by the GUnet governing board.

ca-admin at harica.gr

Greek Academic Network GUnet
National and Kapodestrian University of Athens. – Network Operations Center
University Campus 157 84
Tel: +30-210 7275611
Fax: +30-210 7275601

2.2 Contact Information for support and revocation requests

ca at harica.gr

Hellenic Academic and Research Institutions Certification Authority
Greek Academic Network GUnet
National and Kapodestrian University of Athens. – Network Operations Center
University Campus 157 84

Tel: +30-2310 999000
Fax: +30-2310 999100

3 Certificate types, validation procedures and usage

HARICA issues various types of certificates. All Certificates have a Subject field that contain information for the Subject. This information is validated by HARICA following procedures described in Section 3.2 of the HARICA CP/CPS.

3.1 Certificate types and validation procedures

Subject information is composed according to the certificate type. The Subscriber's name is called a Distinguished Name (DN).

DN Attribute	Interpretation
CN or common name (OID: 2.5.4.3)	If present, for SSL/TLS certificates, this field MUST contain an FQDN that is one of the values contained in the Certificate's subjectAltName extension. For Client, S/MIME or Code Signing certificates, this field MUST contain a representation of the Subject's name. For Client Certificates, "common name" is used for user-friendly representation of the Subject's name to represent itself. This name does not need to be exact match of the fully registered organization name or the person's formal given name and surname.
G or givenName (OID: 2.5.4.42)	Subject's formal given name
SN or surname (OID: 2.5.4.4)	Subject's formal surname
E or emailAddress	Subject's email address
streetAddress (OID: 2.5.4.9)	The physical address of the Subject
postalCode (OID: 2.5.4.17)	The postal code for the physical address
L or Locality (OID: 2.5.4.7)	Postal address City
ST for State or Province Name (OID: 2.5.4.8)	Postal address State or Province
C or Country (OID: 2.5.4.6)	Subject's Country
O or Organization (OID: 2.5.4.10)	Subject's full registered Organization Name
OU or Organizational Unit	Subject Organizational Unit or sub-unit, or special attribute of the signatory depending on the intended use or attributes of the certificate.
serialNumber (OID: 2.5.4.5)	A unique identifier to disambiguate the Subject Name within the context of an Issuing CA
OrganizationIdentifier (OID: 2.5.4.97)	A unique identifier for the Organization

The subject field identifies the entity associated with the Public Key stored in the subject Public Key field. It contains the following:

- Email (E) (Optional for SSL/TLS certificates): The e-mail address of the subject as verified under CP/CPS section 3.2.2.4.2.
- Common Name (OID: 2.5.4.3) (Optional for SSL certificates, Required for Code Signing and Client Certificates): Subject Common Name. If present, for SSL/TLS certificates, this field MUST contain an FQDN that is one of the values contained in the Certificate's subjectAltName extension. For Client, S/MIME or Code Signing certificates, this field MUST contain a representation of the Subject's name as verified under CP/CPS section 3.2.2.1. Common names that also belong to the DNS namespace are forbidden for non-SSL certificates.
- givenName (OID: 2.5.4.42) and surname (OID: 2.5.4.4): Per QCP-n and QCP-n-qscd, contain a representation of the Subject's given name and surname as verified under CP/CPS section 3.2.2.1. Further specifications from ETSI EN 319 412-2 apply.
- streetAddress (OID: 2.5.4.9): The physical address of the Subject as verified under CP/CPS section 3.2.2.1.
- postalCode (OID: 2.5.4.17): The postal code for the physical address of the Subject as verified under CP/CPS section 3.2.2.1.
- 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 (OID: 2.5.4.10): Subject Organization Name as verified under CP/CPS section 3.2.2.1
- Locality (OID: 2.5.4.7) (Optional if "State or Province" is present): Subject Locality as verified under CP/CPS section 3.2.2.1
- State or Province (OID: 2.5.4.8) (Optional if "Locality" is present): Subject State as verified under CP/CPS section 3.2.2.1
- Country (OID: 2.5.4.6): Subject Country as verified under CP/CPS section 3.2.2.1
- 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.
- serialNumber (OID: 2.5.4.5) (Optional): Per QCP-n and QCP-n-qscd, contains a unique identifier to disambiguate the Subject Name within the context of an Issuing CA per ETSI EN 319 412-2. Depending on the Person's decision, one of the following identifiers may be used:
    - Social Security Number with the following semantics: "**PNO**GR-12345678". In this example, GR is the Subject's Country.
    - Personal Identification Card with the following semantics: "**IDC**GR-AK1234567". In this example, GR is the Subject's Country.
    - Tax Identification Number with the following semantics: "**TIN**EL-123456789". Especially for Tax Identifiers, the "country" identifier value should comply with the European Council Directive

2006/112/EC article 215. In this example, EL is the Subject's Country for Greece.
    - Passport Number with the following semantics: "**PAS**GR-1231232". In this example, GR is the Subject's Country.
    - A Unique 10-digit Identifier assigned by HARICA
- OrganizationIdentifier (OID: 2.5.4.97): Per QCP-l and QCP-l-qscd, contains a unique identifier for the Organization per ETSI EN 319 412-3. Depending on the Legal Entity's decision, one of the following identifiers must be used:
    - Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**GR-123456789". In this example, GR is the Subject's Country.
    - Legal Entity's Tax Identification Number with the following semantics: "**VAT**EL-123456789". Especially for Tax Identifiers, the "country" identifier value should comply with the European Council Directive 2006/112/EC article 215. In this example, EL is the Subject's Country for Greece.

3.1.1 SSL/TLS Certificate

By issuing an SSL/TLS Certificate, HARICA represents that it followed the procedures set forth in its CP/CPS to verify that, as of the Certificate's issuance date, all Subject Information was accurate. HARICA shall not include a Domain Name or IP Address in a Subject attribute except as specified in CP/CPS Section 3.2.2.4 or Section 3.2.2.5.

3.1.2 Client/CodeSigning Certificate

By issuing a Client/CodeSigning Certificate, HARICA represents that it followed the procedures set forth in its CP/CPS to verify that, as of the Certificate's issuance date, all Subject Information was accurate. HARICA shall not include a commonName, emailAddress in a Subject attribute except as specified in CP/CPS Section 3.2.3. Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4) are not broadly supported by application software, HARICA may use the subject:organizationName field to convey a natural person Subject's name or DBA.

3.1.3 Certificate for electronic signatures

By issuing a Certificate for electronic signatures under the QCP-n policy or a Qualified Certificate for electronic signatures under the QCP-n-qscd policy, HARICA shall include at least the "commonName", "Country", "givenName" and "surname" attributes in the SubjectDN field. If these attributes are not sufficient to ensure Subject name uniqueness within the context of the Issuing CA, then the serialNumber shall be present.

3.1.4 Certificate for electronic seals

By issuing a Certificate for electronic seals under the QCP-l policy or a Qualified Certificate for electronic seals under the QCP-l-qscd policy, HARICA shall include at least

the “commonName”, “Country”, "organizationName" and "OrganizationIdentifier” attributes in the SubjectDN field.

3.1.5 Time-Stamp Tokens

HARICA also issues Time-Stamp Tokens and Qualified Time-Stamp Tokens. Qualified Time-stamp Tokens comply with Regulation (EU) 910/2014 (eIDAS). Both types of Time-Stamp Tokens provide proof that a datum existed before a point in time.

3.2 Certificate Usage

3.2.1 Appropriate certificate uses

HARICA Certificates can be used for authentication, encryption, access control and digital signing, in all network services and applications in which the required level of security is equal or lower than that of the certificate issuance process.

Typical applications in which digital certificates issued by HARICA can be used, are the following (the list is not restrictive):

a) Signing of an “electronic document” by a natural person or legal entity using a digital certificate and the relevant private key, preferably with the use of a “Secure Signature Creation Device” SSCD or a “Qualified Signature/Seal Creation Device” QSCD (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 signatory to the content of document and the non-repudiation of signature.

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

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

d) “Encryption of documents and messages” with the use of the recipient’s publicly available certificate, ensuring that only she/he, the holder of corresponding private key, can decipher and read the document or the message.

e) Certification of other Trust Service Providers 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/TLS, IPSec etc.

HARICA also operates as a Qualified Time-Stamping Authority providing Qualified and non-Qualified Time-Stamp Tokens. If a TSU issues time-stamps that are claimed to be qualified electronic time-stamps as per Regulation (EU) No 910/2014, this TSU shall not issue non-qualified electronic time-stamps.

3.2.2 Forbidden certificate use

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 or any other uses that are not included in the first paragraph of CP/CPS section 1.4.1

4 Reliance limits

HARICA has no reliance limits other than the ones described in the appropriate and forbidden certificate use stated in Section 3.2.1 and 3.2.2.

The retention period for archived logs is documented in CP/CPS Section 5.5.2.

For the Time-Stamp Tokens, HARICA conforms with requirements set in ETSI EN 319 421 and includes an "`accuracy`" field with a minimum accuracy of one (1) second to a UTC source. If it is detected that the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC, the Time-Stamping Unit shall stop time-stamp issuance.

5 Obligations of Subscribers

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.

6 Certificate status checking obligations of Relying Parties and other obligations

The entities that trust the provided certification services or otherwise called the Relying Parties can be any entity, 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 are the natural 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 HARICA CP/CPS, and after having checked and verified the validity of a certificate that has been issued by HARICA, 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, Relying Parties must check that:

- √ The validity period of the certificate has begun and has not expired.
- √ The certificate is correctly chained to a HARICA Subordinate CA Certificate that chains to one of HARICA's publicly trusted Root CA Certificates.
- √ The certificate was not revoked for any reason when the signing operation occurred.
- √ Subject identification matches the details that the signer presents.
- √ The usage of the certificate matches the intended usage it was issued for, by HARICA.
- √ They abide by the terms and the conditions as described in the HARICA CP/CPS.

The following Representations and Warranties apply to Relying Parties

- ✓ 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.

7 Limited warranty and disclaimer/Limitation 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 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 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 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.

In the event that HARICA deviates from the provisions set forth in its CP/CPS when issuing "**Qualified Certificates for electronic signatures**" and "**Qualified Certificates for electronic seals**", certain liability provisions apply:

- HARICA is only liable for the correct verification of the application and the resultant contents of Qualified Certificates (with the exception of the "OU" field as stated in 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 Qualified 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 Qualified Certificate or if the Subscriber uses the Qualified Certificate in an incorrect way.
- With the exception of the previous cases, HARICA's maximum aggregate liability under this CP/CPS 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. This is covered via a Professional Liability Insurance contract between HARICA and a major Insurance Company.

7.1 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.

8 Applicable agreements, CPS, CP

See the HARICA CP/CPS at https://www.harica.gr/documents/CPS

9 Privacy Policy

9.1 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.

9.2 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.

9.3 Responsibility to protect private information

All private and personal information handled and processed by HARICA, is in accordance to 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.

9.4 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.

10 Refund policy

Not defined

11 Applicable law, complaints and dispute resolution

This Certification Policy and Certification Practice Statement of HARICA Public Key Infrastructure shall be interpreted, construed and enforced in all respects in accordance with the applicable European and Greek legislation. All proceedings or legal action arising from Certification Policy and Certification Practice Statement of HARICA Public Key Infrastructure must be commenced in the exclusive jurisdiction of courts of Athens Greece.

If a dispute or difference arises in connection with, or out of the interpretation of the Certificate Policy/Certification Practice Statement and the operations of the Certification Authority then the Subscriber concerned 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.

Unless settled amicably, any disputes in connection with or arising out of this Certification Policy and Certification Practice Statement of HARICA Public Key Infrastructure shall be referred and submitted to the Greek courts that are competent and the exclusive venue is Athens Greece

12 TSP and repository licenses, trust marks and audit

HARICA PKI meets the specifications of:

- ETSI EN 319 411-1 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing certificates; Part 1: General Requirements*",
- ETSI EN 319 411-2 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*",
- ETSI EN 319 421 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing Time-Stamps*",
- 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"*,
- Precedential Decree 150/2001 and
- Regulation (EU) No 910/2014 (e-IDAS) of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

HARICA 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).

HARICA is annually audited by an accredited Conformance Assessment Body. Audit reports are submitted to Application Software Suppliers and National Supervisory Bodies. A summary of these reports is also available at https://www.harica.gr.