Audit Attestation for

Hellenic Academic & Research Institutions Certification Authority ("HARICA")

Reference: No. 150621-06-AL

Thessaloniki, 2021-06-15

To whom it may concern,

This is to confirm that QMSCERT has audited the CAs of the GREEK UNIVERSITIES NETWORK (dba "GUNET"), owner of HELLENIC ACADEMIC & RESEARCH INSTITUTIONS CERTIFICATION AUTHORITY ("HARICA"), without findings.

This present Audit Attestation Letter is registered under the unique identifier number "150621-06-AL" and consists of 8 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

QMSCERT
90, 26th October Str.
546 27 Thessaloniki, Greece
E-Mail: ict-certification@qmscert.com
Phone: +30 2310 443041

With best regards,

Lazaros Karanikas
Digitally signed by Lazaros Karanikas
Date: 2021.06.15 15:53:47 +03'00'

Lazaros Karanikas
Managing Director

Identification of the conformity assessment body (CAB) and assessment organization:	• QMSCERT 26th October Str., 90 546 27 Thessaloniki Greece • Registered under nº 042094606000 • Accredited by ACCREDIA under registration 272B[1] for the certification of trust services according to "EN ISO/IEC 17065:2013" and "ETSI EN 319 403 V2.2.2 (2015-08)". • Insurance Carrier: AIG Europe S.A., Policy No. P2301004773 • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team:	• Number of team members: Two (2) • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: All team members have knowledge of: 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and

[1] https://services.accredia.it/ppsearch/accredia_orgmask.jsp?ID_LINK=1733&area=310&PPSEARCH_ORG_SEARCH_MASK_ORG=3761&PPSEARCH_ORG_SEARCH_MASK_SCHEMI=&PPSEARCH_ORG_SEARCH_MASK_SCHEMI_ALTRI=&PPSEARCH_ODC_SEARCH_MASK_SETTORE_ACCR=&PPSEARCH_ORG_SEARCH_MASK_CITTA=&PPSEARCH_ORG_SEARCH_MASK_PROVINCIA=&PPSEARCH_ORG_SEARCH_MASK_REGIONE=&PPSEARCH_ORG_SEARCH_MASK_STATO=&orgtype=all&PPSEARCH_ORG_SEARCH_MASK_SCOPO=&PPSEARCH_ORG_SEARCH_MASK_PDFACCREDITAMENTO=&submitBtn=Cerca

	interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: none. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. • Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing	• Number of Reviewers/Audit Quality Managers involved independent from the audit team: One (1)

audit quality management:	• The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the trust service provider (TSP):	GREEK UNIVERSITIES NETWORK (“GUNET”) Network Operation Center, National and Kapodistrian University of Athens, Panepistimioupoli Ilissia 157 84 Athens Greece Registered under 13392/28-9-2000

Audit type:	Period of Time (full audit)
Audit period covered for all policies:	2021-02-19 to 2021-04-29
Audit dates:	2021-03-22 to 2021-03-24 (remote) 2021-03-23 (on site)
Audit locations:	MR1, Thessaloniki, Greece (operations) MR4, Thessaloniki, Greece (disaster recovery)

Identification of the audited Root-CA:	HARICA Client RSA Root CA 2021	
	Distinguished Name	C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA Client RSA Root CA 2021
	SHA-256 fingerprint	1BE7ABE30686B16348AFD1C61B6866A0EA7F4821E67D5E8AF937CF8011BC750D
	Certificate Serial number	5552F81EDB1B242C9EBB9618CD02283E
	Applied policy	ETSI EN 319 411-1 V1.2.2: LCP, NCP, NCP+
	Technical constraints	-

The audit was performed according to the European Standards “ETSI EN 319 411-1, V1.2.2 (2018-04)” and “ETSI EN 319 401, V2.2.1 (2018-04)” as well as CA Browser Forum Requirements “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.7.3”, considering the requirements of the “ETSI EN 319 403-1 V2.3.1 (2020-06)” and “ETSI TS 119 403-2 V1.2.4 (2020-11)” for the Trust Service Provider Conformity Assessment.

The full annual audit was based on the following policy and practice statement documents of the TSP:

1. [CP/CPS] Certificate Policy/ Certification Practice Statement, version 4.3, dated 2021-02-18[2]

No major or minor non-conformities have been identified during the audit.

No public incidents have been documented in the audit period for the hierarchy of Sub-CAs which chain up to the scoped Root-CA.

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CAs that are technically capable of issuing client and server authentication, code signing, time-stamping, document signing or email protection certificates and that have been issued by this Root-CA are in the scope of regular audits.

[2] Other policy and practice statement documents of the TSP within the scope of the audit:
1. [CP/CPS] Certificate Policy/ Certification Practice Statement, version 4.2, dated 2020-09-30
2. [CP/CPS] Certificate Policy/ Certification Practice Statement, version 4.1, dated 2020-08-11
3. [CP/CPS] Certificate Policy/ Certification Practice Statement, version 4.0, dated 2020-03-31

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN=HARICA Client Authentication RSA,O=Hellenic Academic and Research Institutions CA,C=GR	858D7018873D31678AA155D071B3E0F2E09025169DD7938ECE98CAB81034A81D	ETSI EN 319 411-1: LCP, NCP, NCP+	TLS Web Client Authentication
CN=HARICA S/MIME RSA,O=Hellenic Academic and Research Institutions CA,C=GR	B13EC301E7BFE1DDB9C5BFC071DC29C55E82EE933273A23134946FBDFD3ACE63	ETSI EN 319 411-1: LCP, NCP, NCP+	TLS Web Client Authentication, E-mail Protection

Table 1: Sub-CA's issued by the Root-CA or its Sub-CA's

Modifications record

Version	Issuing Date	Changes
Version 1	2021-06-15	Initial attestation

End of the audit attestation letter.