



Audit Attestation for

Hellenic Academic & Research Institutions Certification Authority (“HARICA”)

Reference: No. 280622-04-AL

Thessaloniki, 2022-06-28

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 “280622-04-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
Managing Director

Seat
90, 26th October Str.,
546 27, Thessaloniki
Greece

Operations
28, Vlasiou Gavriilidi Str.
546 55, Thessaloniki
Greece

Contact information
Tel. +30-2310-535-198
Fax. +30-2310535-008
Email: info@qmscert.com
<http://www.qmscert.com>

<p>Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:</p>	<ul style="list-style-type: none"> • QMSCERT 26th October Str., 90 546 27 Thessaloniki Greece Registered under n° 042094606000 • Accredited by ACCREDIA under registration 272B¹ for the certification of trust services according to “EN ISO/IEC 17065:2013” and “ETSI EN 319 403 V2.2.2 (2015-08)” and/or “ETSI EN 319 403-1 V2.3.1 (2020-06)” respectively. • Insurance Carrier (BRG section 8.2): AIG Europe S.A., Policy No. P2301004773 • Third-party affiliate audit firms involved in the audit: None.
<p>Identification and qualification of the audit team:</p>	<ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 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. <p>Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and</p>

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_ORG_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

	<p>interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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.
<p>Identification and qualification of the reviewer performing</p>	<ul style="list-style-type: none"> • Number of Reviewers/Audit Quality Managers involved independent from the audit team: One (1)

audit quality management:	<ul style="list-style-type: none"> 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 CA / Trust Service Provider (TSP):	<p>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</p>
Type of audit:	<input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input checked="" type="checkbox"/> Period of time, full audit
Audit period covered for all policies:	2021-03-30 to 2022-03-29
Point in time date:	none, as audit was PoT audit
Audit dates:	2022-03-28 to 2022-04-05 (on site)
Audit locations:	MR1, Thessaloniki, Greece (operations) MR4, Thessaloniki, Greece (disaster recovery)
Standards considered:	<p>European Standards:</p> <input checked="" type="checkbox"/> ETSI TS 119 495 V1.5.1 (2021-04) <input type="checkbox"/> ETSI EN 319 421 V1.1.1 (2016-03) <input checked="" type="checkbox"/> ETSI EN 319 411-2, V2.4.1 (2021-11) <input checked="" type="checkbox"/> ETSI EN 319 411-1, V1.3.1 (2021-05) <input checked="" type="checkbox"/> ETSI EN 319 401, V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <input checked="" type="checkbox"/> EV SSL Certificate Guidelines, version 1.7.8 <input checked="" type="checkbox"/> Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.8.2 <input type="checkbox"/> Baseline Requirements for the Issuance and Management of Code Signing Certificates, version 2.7 <p>For the Trust Service Provider Conformity Assessment:</p> <input checked="" type="checkbox"/> ETSI EN 319 403-1 V2.3.1 (2020-06) <input checked="" type="checkbox"/> ETSI TS 119 403-2 V1.2.4 (2020-11)

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

1. [\[CP/CPS\]](#) Certificate Policy/ Certification Practice Statement, version 4.5, dated 2022-03-23
2. [\[CP/CPS\]](#) Certificate Policy/ Certification Practice Statement, version 4.4, dated 2021-05-21
3. [\[CP/CPS\]](#) Certificate Policy/ Certification Practice Statement, version 4.3, dated 2021-02-18

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

No incidents have been reported or remain open within the audit period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	Technical constraints
CN=HARICA TLS RSA Root CA 2021,O=Hellenic Academic and Research Institutions CA,C=GR	D95D0E8EDA79525BF9BEB11B14D2100D3294985F0C62D9FABD9CD999ECCB7B1D	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP; ETSI EN 319 411-2: QCP-w; ETSI TS 119 495: QCP-w-psd2	not defined

Table 1: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN=HARICA DV TLS RSA,O=Hellenic Academic and Research Institutions CA,C=GR	28101EE3CD2FF6F225FBF0EDE94AB50D6762AFDBAB964F7C9D3CCF7F02EE9838	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP	TLS Web Client Authentication, TLS Web Server Authentication
CN=HARICA EV TLS RSA,O=Hellenic Academic and Research Institutions CA,C=GR	CA623354A31C7878815E0D901FA47E30D10A61F6945D3CBEFC4757F447FA8AEA	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP	TLS Web Client Authentication, TLS Web Server Authentication
CN=HARICA IV TLS RSA,O=Hellenic Academic and Research Institutions CA,C=GR	1DF929D90B3AD4EF94D36402F483462E8CB678495C687022423545B19E2F0615	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP	TLS Web Client Authentication, TLS Web Server Authentication

CN=HARICA OV TLS RSA,O=Hellenic Academic and Research Institutions CA,C=GR	9FBD886945FB6CB63EEBF11077DAC980E45368D2458BA5EF0A8D727046FCD292	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP	TLS Web Client Authentication, TLS Web Server Authentication
CN=HARICA EV TLS RSA 2,O=Hellenic Academic and Research Institutions CA,C=GR	75E328643BFE7642DD840E3169F942C66BF04919D8A7FB0AF96602612003C3E3	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP	TLS Web Client Authentication, TLS Web Server Authentication

Table 2: Sub-CA's issued by the Root-CA or its Sub-CA's in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2022-06-28	Initial attestation

End of the audit attestation letter.