Audit Attestation for

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

Reference: No. 150621-03-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 "150621-03-AL" and consists of 9 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 15:52:52 +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:	2020-03-30 to 2021-03-29
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:	Hellenic Academic and Research Institutions ECC RootCA 2015	
	Distinguished Name	C=GR/L=Athens/O=Hellenic Academic and Research Institutions Cert. Authority/CN=Hellenic Academic and Research Institutions ECC RootCA 2015
	SHA-256 fingerprint	44B545AA8A25E65A73CA15DC27FC36D24C1CB9953A066539B11582DC487B4833
	Certificate Serial number	0
	Applied policy	ETSI EN 319 411-1 V1.2.2: LCP, NCP, NCP+, DVCP, OVCP, IVCP, EVCP ETSI EN 319 411-2 V2.2.2: QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, QCP-w ETSI TS 119 495 V1.4.1: QCP-w-psd2 ETSI EN 319 421 V1.1.1: BTSP
	Technical constraints	-

The audit was performed according to the European Standards “ETSI TS 119 495 V1.4.1 (2019-11)”, “ETSI EN 319 421 V1.1.1 (2016-03)”, “ETSI EN 319 411-2, V2.2.2 (2018-04)”, “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 “EV SSL Certificate Guidelines, version 1.7.4”, “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.7.3” and “Baseline Requirements for the Issuance and Management of Code Signing Certificates, version 2.1”, 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.

This Audit Attestation also covers the following incidents as documented under

- Bug 1649945, HARICA: Incorrect OCSP Delegated Responder Certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1649945
- Bug 1651465, HARICA: Delayed revocation for non-BR-compliant CA Certificates within 7 days: https://bugzilla.mozilla.org/show_bug.cgi?id=1651465
- Bug 1699796, HARICA: Certificates with invalid policy tree: https://bugzilla.mozilla.org/show_bug.cgi?id=1699796

The remediation measures taken by HARICA as described on Bugzilla (see links above) have been checked by the auditors and properly addressed the incidents. The long-term effectiveness of the measures will be rechecked at the next regular audit.

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 Code Signing ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	013932465EE4FC2448D0C9AEEEA049DE9063AF5E773E8A501AB626F0957E1345	ETSI EN 319 411-1: NCP, NCP+, OVCP, IVCP, EVCP	Code Signing
CN=HARICA Client Authentication ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	4D63F8747A9680F81882B62D0FA993C33581D314C5B596FA373DF92B2C65D4FF	ETSI EN 319 411-1: LCP, NCP, NCP+	TLS Web Client Authentication
CN=HARICA Qualified Legal Entities ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	DD5BAC4F1BB5356AE98D3F0C8E24C59DF84199A56F78F1C161196AAD70283094	ETSI EN 319 411-2: QCP-l-qscd, QCP-l	TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311 .10.3.12
CN=HARICA Qualified Natural Entities ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	4D961AEE0D2DD0ADF433B4AAC261CE5871665CF39FCA1B4838AE6620DA685046	ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311 .10.3.12
CN=HARICA S/MIME ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	9CD07290E8BEDD99CF7397F94CB012B22EEC13DA52ED94F3017A2EA4146EA98D	ETSI EN 319 411-1: LCP, NCP, NCP+	TLS Web Client Authentication, E-mail Protection
CN=HARICA SSL ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	11D5EF460DAB3582B742123127127D54040FB1C206E26F025CB58458F225111A	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP; ETSI EN 319 411-2: QCP-w	TLS Web Client Authentication, TLS Web Server Authentication

CN=HARICA Administration Client ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR **(REVOKED AT 2020-09-03)**	7A52945F5902D53C0DB76A200EB9F85C7C424B23F939FFE140C5DBD0B1F2C7D8	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311.10.3.12, OCSP Signing
CN=HARICA Administration SSL ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	3E1479804765A62BB7BD4F0DDEBB55A946A2063CD2882F05461B1754F1B667B1	ETSI EN 319 411-1: DVCP, OVCP, IVCP, EVCP	TLS Web Client Authentication, TLS Web Server Authentication
CN=HARICA EV Code Signing ECC SubCA R1,O=Hellenic Academic and Research Institutions CA,L=Athens,C=GR	523EC59EC9E637E635F8BE2954D56D7624371B10BAEC6D123C11D84BFD7D5261	ETSI EN 319 411-1: NCP+, EVCP	Code Signing
CN=HARICA EV TLS ECC SubCA R1,O=Hellenic Academic and Research Institutions CA,L=Athens,C=GR	701EB23F95564CD5569CD20E5F05C2888900BAE9BA03ABF5ABE57BFE04B54A60	ETSI EN 319 411-1: EVCP	TLS Web Client Authentication, TLS Web Server Authentication
CN=HARICA QWAC ECC SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),L=Athens,C=GR	BA0312F7B72F6B64B4CCEE34B5F628CF65A1F3B9F16B8DFE7ADA90C54E475A1C	ETSI EN 319 411-1: OVCP, EVCP; ETSI EN 319 411-2: QCP-w, QCP-w-psd2	TLS Web Client Authentication, TLS Web Server Authentication
CN=HARICA Administration Client ECC SubCA R3,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	978011D478E7BC4C3BCBB2F2659759278AA41A17F53F0AED132726281CE34BAF	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311.10.3.12

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.