



SMIME BR Audit Attestation for Hellenic Academic & Research Institutions Certification Authority (“HARICA”)

Reference: 270625-08-AL

Thessaloniki, 2025-06-27

To whom it may concern,

This is to confirm that “QMSCERT Audits Inspections Certifications S.A. (Q-CERT S.A.)” 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 “270625-08-AL” covers multiple Root-CAs and consists of 24 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Q-CERT S.A.
28, Vlasίου Gavrielidi Str.
546 55 Thessaloniki, Greece
E-Mail: ict-certification@qmscert.com
Phone: +30 2310 443041

With best regards,

Eleni Bakirtzi
Head of Conformity Assessment Body

Seat
28, Vlasίου Gavrielidi Str.
546 55, Thessaloniki
Greece

Operations
28, Vlasίου Gavrielidi Str.
546 55, Thessaloniki
Greece

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

General audit information

<p>Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor</p>
<ul style="list-style-type: none"> • QMSCERT Audits Inspections Certifications S.A. (Q-CERT S.A.), 28 Vlassiou Gavrielidi Str., 546 55, Thessaloniki, Greece, registered under n° 042094606000 • Accredited by ACCREDIA under registration no. 01326¹ for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403 V2.2.2 (2015-08)" / "ETSI EN 319 403-1 V2.3.1 (2020-06)". • 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 interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic.</p> • 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:

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

This attestation is based on the template v3.3 as of 2024-10-08, that was approved for use by ACAB-c.

- 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 audit quality management

- Number of Reviewers/Audit Quality Managers involved independent from the audit team: Two (2)
- 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):	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
--	--

Type of audit:	<input checked="" type="checkbox"/> Period of time, full audit
----------------	--

Audit period covered for all policies:	2024-03-30 to 2025-03-29
--	--------------------------

Point in time date:	none, as audit was a period of time audit
Audit dates:	2025-03-28 (remote) 2025-04-03 to 2025-04-14 (on site)
Audit location:	KEDEK, Thessaloniki, Greece (operations) MR1, Thessaloniki, Greece (operations) MR4, Thessaloniki, Greece (disaster recovery)

Root 1: Hellenic Academic and Research Institutions RootCA 2011

Standards audited:	<p>European Standards:</p> <ul style="list-style-type: none"> • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"> • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 1.7 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"> • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)
--------------------	---

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

- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.9, as of 2025-03-14
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.8, dated 2024-07-17
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.7, as of 2023-07-17

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

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Hellenic Academic and Research Institutions RootCA 2011,O=Hellenic Academic and Research Institutions Cert. Authority,C=GR	BC104F15A48BE709DCA542A7E1D4B9DF6F054527E802EAA92D595444258AFE71	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

Table 1: Root-CA 1 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
CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR [Cross-Certificate]	F28A97AC28CFED10A93A7F078F978C8F6204C9D8451F745D5FEBBD6E0B6D4D7C	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=Academy of Athens Client CA R1,O=Academy of Athens,L=Athens,C=GR	DDAA5F72E10FD3AD072AD2C0D21958DBF1709E7AED13B38C264728FCE5C9BA1E	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=Institute of Accelerating Systems and Applications Client CA R1,O=Institute of Accelerating Systems and Applications,L=Athens,C=GR	DC1AB1EFCA2083FE1EA6D0D3DC4A7879D5CC6D3DA3F0A81E94C8699D3AA7CB0E	ETSI EN 319 411-1: NCP, NCP+ amended by ETSI TS 119 411-6
CN=Ionian University Client CA R1,O=Ionian University,L=Kerkyra,C=GR	C95A9426410E11E70EED947806FD87F6F0DE77B98F1C454BE10D35C4442DC1DD	ETSI EN 319 411-1: NCP, NCP+ amended by ETSI TS 119 411-6
CN=HARICA S/MIME RSA SubCA R1,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	E530511259D33FB3EDD38E0E799FF9E8F99D4DB2DA0DEE08EAF5A6D15CCE9BFC	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

This attestation is based on the template v3.3 as of 2024-10-08, that was approved for use by ACAB-c.

CN=HARICA Client Authentication RSA SubCA R1,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	D25B6C50594F6119DC3AB2E59F5509FC904F10C4FFA757C0129EEBDA86BFFCB1	[Technically-constrained non-Email Protection CA]
--	--	--

Table 2: Sub-CA's issued by the Root-CA 1 or its Sub-CA's in scope of the audit

Root 2: Hellenic Academic and Research Institutions RootCA 2015

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none"> • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"> • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 1.7 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"> • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)
-----------------------	---

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

- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.9, as of 2025-03-14
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.8, dated 2024-07-17
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.7, as of 2023-07-17

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

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	A040929A02CE53B4ACF4F2FFC6981CE4496F755E6D45FE0B2A692BCD52523F36	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

Table 3: Root-CA 2 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
CN=Hellenic Academic and Research Institutions Code Signing CA R1,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	68494D765B5E71404F56D06A1A853A27C369B96B7D405EED9BD79E0FC308EB0F	[Technically-constrained non-Email Protection CA]
CN=HARICA S/MIME RSA SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	5C97E0FD1EBD6E136A71626F860AB5D65B797E7ED3C1C1BF4E653822375A4644	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=HARICA Client Authentication RSA SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	15DACB49F048B95408A0EEC6891729D9235CCAE32F45CFDA07175402BEE78300	[Technically-constrained non-Email Protection CA]
CN=HARICA Qualified Legal Entities SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	CDF27EEA0C3A5512369108FD74635D2D4CF50E94D6CA199BED7DE81B0D09A336	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=HARICA Qualified Natural Entities SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	094F78C53EC5D8082BC5D5AAD1B11D5DF952BE56933358DBF5963542913A50CD	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

This attestation is based on the template v3.3 as of 2024-10-08, that was approved for use by ACAB-c.

CN=Aristotle University of Thessaloniki SSL RSA SubCA R2,O=Aristotle University of Thessaloniki,L=Thessaloniki,C=GR	0EE82CEB7ECA241CCC29D4E588062C43E447EDE6C696F135ACC411966126BA83	[Technically-constrained non-Email Protection CA]
CN=Academy of Athens SSL SubCA R2,O=Academy of Athens,L=Athens,C=GR	DC9455CA47F5FD9BF3BBABBEACF88F3DEB3B58BFA85AF404DFD21617CE90A0DD	[Technically-constrained non-Email Protection CA]
CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2,O=University Ecclesiastical Academy of Vella of Ioannina,L=Ioannina,C=GR	CDFF27AFA3DAF9F706AA7AC530298337E520C8B10A22F6514E00E21FD2873B79	[Technically-constrained non-Email Protection CA]
CN=GRnet SSL RSA SubCA R2,O=Greek Research and Technology Network,L=Athens,C=GR	C161F5AADE40FBC9723F0892DE963D4D10405561A6BDC69A72798F918BED19CD	[Technically-constrained non-Email Protection CA]
CN=HARICA SSL RSA SubCA R3,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	70B6A10C0CA76DECE7ADBE970B76A37D8A02857B134C7505B184EBD5FCA4F3EA	[Technically-constrained non-Email Protection CA]
CN=HARICA Qualified Legal Entities SubCA R3,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	C6CB08B5D6DFE461AECE9AA3CF03AF7FED1341C9E6EE0052129C27CA754933F2	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=HARICA Qualified Natural Entities SubCA R3,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ADDBE88B468154CF8F7773288C8C50F760879E490892AA9272815B814E721E7D	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=HARICA S/MIME RSA SubCA R3,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	593C4AB6066CDF6185067F562677FDFF533656DB4BD2D577735301704150218	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=GRNET TLS RSA SubCA R1,O=National Infrastructures for Research and Technology,L=Athens,C=GR	88CE49E3A4FA37EAE28E8E35F8FF8CF7568CA845639CEF3B8DFDF4E4693AC14A	[Technically-constrained non-Email Protection CA]

This attestation is based on the template v3.3 as of 2024-10-08, that was approved for use by ACAB-c.

CN=International Hellenic University TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	9C782F6B0558ADCB1CC9EF845320D14592C9220FCF0030C0980D9D753B06624F	[Technically-constrained non-Email Protection CA]
CN=University of Ioannina TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	46727B90C5A5F73375082D9B1BC9F17B445F5020A95E37DFDF1EF20B287C5115	[Technically-constrained non-Email Protection CA]
CN=University of Patras TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	673E34D7E1E6B25C187F391CC49138B4722A907E33F5B7487B613BB6DFE78909	[Technically-constrained non-Email Protection CA]
CN=National Technical University of Athens TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	1E8F051F2226F992D17B7CF17F0DECE0AA769902E9FE8D11F35B19B18A5A14F1	[Technically-constrained non-Email Protection CA]
CN=University of the Aegean TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	7E2C537397E7B8D9B24D87F304C96EA057A407CE11D0B66D99BA4B8A22BB1167	[Technically-constrained non-Email Protection CA]
CN=HARICA EV Code Signing RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,L=Athens,C=GR	0324BF1DE988B39D2A86F6A217B21940D631EFB746898E838C49120DA63749AC	[Technically-constrained non-Email Protection CA]
CN=HARICA EV TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,L=Athens,C=GR	F628264C79DBFBDFCFDEC643171BDCBD4DE7483F9C80EA59068887AE449A2E48	[Technically-constrained non-Email Protection CA]
CN=HARICA QWAC RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),L=Athens,C=GR	DAB3FA0D6E821006FE709AE12176ABA2F397706CC9C71F5C1C0D098044DAEBDC	[Technically-constrained non-Email Protection CA]

CN=Athens University of Economics and Business TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	3995B01A17800AECF5480E939D9DA44EDCCC7CF2935657C6179D5A1EFA25D74D	[Technically-constrained non-Email Protection CA]
CN=CEDEFOP TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	44CE97F5C957DD056D44C3E1BDFCEB2CF9A7B428ED089839264336303BCAC7EF	[Technically-constrained non-Email Protection CA]
CN=Democritus University of Thrace TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	220040DDA377C944429E8CE913B7D81B36DE34EBF2DC218D2066393D94863439	[Technically-constrained non-Email Protection CA]
CN=Greek Universities Network TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	DC9993DC33A71FD95808787D19A4B55704E601D57EBCEACC8802C78B5C36F5C7	[Technically-constrained non-Email Protection CA]
CN=HEAL-LINK Hellenic Academic Libraries Link TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	8C0994B2AED0085FE542813EE03C4B2D732ECDCC257AE6453114C6C875933BD4	[Technically-constrained non-Email Protection CA]
CN=Harokopio University TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	BA425122F31D9BAE7CBE1E7FA2FF437ADF283E014333485F7691CB856AEC776A	[Technically-constrained non-Email Protection CA]
CN=Inst. of Accelerating Systems and Applications TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	146C1CF9BB7D231060D0FABD986E9850F00501F5A3B7B6AC42C51B38C8E22A23	[Technically-constrained non-Email Protection CA]
CN=Ionian University TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	DA0C4981F6336E06C129F7E8143B2A54AA85A14A63CA44FCE2CDDC69EEE788C9	[Technically-constrained non-Email Protection CA]
CN=Panteion Univ. of Social and Political Sciences TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	F0043E9FEFB37AEA794E690437DC239D6BD2C5CA0FB58A12244555A1A8A2A01A	[Technically-constrained non-Email Protection CA]

This attestation is based on the template v3.3 as of 2024-10-08, that was approved for use by ACAB-c.

CN=Greek School Network TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	CFDFEF037CFDBD6BB0E311E9BB281CA60271C5DAE2695312033806FA4B0E94B7	[Technically-constrained non-Email Protection CA]
CN=Technical University of Crete TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	1AF8B4D49C5A7B6DA536DEA92FDFAF45736205AFCA2DAFFFAECB712DA9C3EBD1	[Technically-constrained non-Email Protection CA]
CN=University of Piraeus TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	25EED131D7193597E48D4E36536CC5CFFBF9EB2042C62573AE8968D8A3695F1C	[Technically-constrained non-Email Protection CA]
CN=National and Kapodistrian University of Athens TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	1744B474101FE6A91936F5E60307C63DA58B88405B045323DEC8C8C00176AF77	[Technically-constrained non-Email Protection CA]
CN=University of Crete TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	5DABDA046272EEC89ECB95A6297DBA910D0144F7EEB5814D073AE54A4A8CF646	[Technically-constrained non-Email Protection CA]
CN=University of Macedonia TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	6539235A5A1F94180C5233EAF8A5D67102DEAA16C0751AEF35B3E67CE5607F29	[Technically-constrained non-Email Protection CA]
CN=University of the Peloponnese TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	1C9D3E8E0CF1E4F39C734D19E479AE971FC3066C000353A2B6AF32795A97EA1B	[Technically-constrained non-Email Protection CA]
CN=University of Western Macedonia TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	EFB44844F37EE6DE3FB4CC8D2C0C832FC8FEEBA9506237E0D1FC7AD4574A4CCA	[Technically-constrained non-Email Protection CA]

CN=HARICA Qualified Time Stamping RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	1D3BDB9882F3D16AD807903DA797EC4ABAC27365D9B3C9B0E227B6B7E265972A	[Technically-constrained non-Email Protection CA]
CN=University of West Attica TLS RSA SubCA R1,O=Hellenic Academic and Research Institutions CA,C=GR	1E3349CD366A93E59EF4152A1E483DAC6076184C5D46D4CDA00E6093EFC9E6A3	[Technically-constrained non-Email Protection CA]
CN=HARICA Institutional Client SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	FEE2CD981C00C5CF3B0A47F3F4BC5DB1E6F4307AD45CE78F998F9BCBD82478EA	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=Greek Federation of Judicial Officers Client RSA SubCA R4,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	8884A7E1A5E7FED19E60E3598E10EF2105ADFF02A0B91DF227069097F9DFDB62	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=Ministry of Digital Governance (Hellenic Republic) SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	6014F88C181CA075E2F7B82A1F518FA604A22486ABB72A76591962FB08646C63	[Technically-constrained non-Email Protection CA]
CN=HARICA TLS RSA Root CA 2021,O=Hellenic Academic and Research Institutions CA,C=GR [Cross-Certificate]	4ACD8DC6020A545A858943A553B5E0F3FC5B859AEA1746650D69CF1210F956D8	[Technically-constrained non-Email Protection CA]

CN=HARICA Institutional TLS RSA,O=Hellenic Academic and Research Institutions CA,C=GR	C5B4ABBD3BAE38114A3A823A8AC4CD31C45465B7C1CEBD84F36D72054AFBE8BB	[Technically-constrained non-Email Protection CA]
CN=ACER Client RSA SubCA R3,O=Agency for the Cooperation of Energy Regulators,L=Ljubljana,C=SI	B8355501E3658AAA20986EFB67A1064ED9E9ACE94CA9E87C8BEE93946E0333E6	[Technically-constrained non-Email Protection CA]
CN=HARICA Code Signing RSA 2,O=Hellenic Academic and Research Institutions CA,C=GR	9B92D7AA0D29B18AFE9E7A66A1BB1A332361B5EE061964A2FC12085093C0D799	[Technically-constrained non-Email Protection CA]
CN=HARICA Time-stamping Certificates RSA 2,O=Hellenic Academic and Research Institutions CA,C=GR	668A4E057F27DF063D0D37C0A6142AAAF786F405DFC5A30F7A7DD5B02DD5A922	[Technically-constrained non-Email Protection CA]
CN=HARICA Code Signing RSA Root CA 2021,O=Hellenic Academic and Research Institutions CA,C=GR [Cross-Certificate]	2EDB3472C14ABB088840B8CD3EA70A65A620F4D2C54A05291DA786F685AFE8F4	[Technically-constrained non-Email Protection CA]

Table 4: Sub-CA's issued by the Root-CA 2 or its Sub-CA's in scope of the audit

Root 3: Hellenic Academic and Research Institutions ECC RootCA 2015

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none"> • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"> • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 1.7 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"> • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)
-----------------------	---

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

- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.9, as of 2025-03-14
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.8, dated 2024-07-17
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.7, as of 2023-07-17

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

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Hellenic Academic and Research Institutions ECC RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	44B545AA8A25E65A73CA15DC27FC36D24C1CB9953A066539B11582DC487B4833	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

Table 5: Root-CA 3 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
CN=HARICA Code Signing ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	013932465EE4FC2448D0C9AEEDA049DE9063AF5E773E8A501AB626F0957E1345	[Technically-constrained non-Email Protection CA]
CN=HARICA Client Authentication ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	4D63F8747A9680F81882B62D0FA993C33581D314C5B596FA373DF92B2C65D4FF	[Technically-constrained non-Email Protection CA]
CN=HARICA Qualified Legal Entities ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	DD5BAC4F1BB5356AE98D3F0C8E24C59DF84199A56F78F1C161196AAD70283094	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=HARICA Qualified Natural Entities ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	4D961AEE0D2DD0ADF433B4AAC261CE5871665CF39FCA1B4838AE6620DA685046	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
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+ amended by ETSI TS 119 411-6

This attestation is based on the template v3.3 as of 2024-10-08, that was approved for use by ACAB-c.

CN=HARICA SSL ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	11D5EF460DAB3582B742123127127D54040FB1C206E26F025CB58458F225111A	[Technically-constrained non-Email Protection CA]
CN=HARICA Administration SSL ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	3E1479804765A62BB7BD4F0DDEBB55A946A2063CD2882F05461B1754F1B667B1	[Technically-constrained non-Email Protection CA]
CN=HARICA EV Code Signing ECC SubCA R1,O=Hellenic Academic and Research Institutions CA,L=Athens,C=GR	523EC59EC9E637E635F8BE2954D56D7624371B10BAEC6D123C11D84BFD7D5261	[Technically-constrained non-Email Protection CA]
CN=HARICA EV TLS ECC SubCA R1,O=Hellenic Academic and Research Institutions CA,L=Athens,C=GR	701EB23F95564CD5569CD20E5F05C2888900BAE9BA03ABF5ABE57BFE04B54A60	[Technically-constrained non-Email Protection CA]
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	[Technically-constrained non-Email Protection CA]
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: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=HARICA TLS ECC Root CA 2021,O=Hellenic Academic and Research Institutions CA,C=GR [Cross-Certificate]	50E27F90EB6AF495B0E6EEB655CC89444C27D3C95B6823FA02ABDC95F1636AE1	[Technically-constrained non-Email Protection CA]
CN=HARICA Institutional TLS ECC,O=Hellenic Academic and Research Institutions CA,C=GR	B67E4E92286E168A916F3DBCADC3F0B83DBC0ADBE43F995C1FAAD316DDEC75D8	[Technically-constrained non-Email Protection CA]

This attestation is based on the template v3.3 as of 2024-10-08, that was approved for use by ACAB-c.

CN=HARICA Code Signing ECC 2,O=Hellenic Academic and Research Institutions CA,C=GR	F2CB382030F2910E8D5E4D1BA98992AFA7635BFECB5F76BEF53FD822ED691F0E	[Technically-constrained non-Email Protection CA]
CN=HARICA Code Signing ECC Root CA 2021,O=Hellenic Academic and Research Institutions CA,C=GR [Cross-Certificate]	AC70544B35F91FB5CAD41698ABDD6825FCDEBDF6E082100190B8F1F437F92195	[Technically-constrained non-Email Protection CA]

Table 6: Sub-CA's issued by the Root-CA 3 or its Sub-CA's in scope of the audit

Root 4: HARICA Client RSA Root CA 2021

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none"> • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"> • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 1.7 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"> • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)
-----------------------	---

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

- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.9, as of 2025-03-14
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.8, dated 2024-07-17
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.7, as of 2023-07-17

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

This Audit Attestation also covers the following incidents as described in the following.

- Bug #1942130, HARICA: S/MIME certificate issuance without proper validation: https://bugzilla.mozilla.org/show_bug.cgi?id=1942130.
- Bug #1943596, HARICA: S/MIME certificate issuance with incorrect commonName: https://bugzilla.mozilla.org/show_bug.cgi?id=1943596.
- Bug #1945389, HARICA: delayed revocation for bug 1943596: https://bugzilla.mozilla.org/show_bug.cgi?id=1945389.

The remediation measures taken by HARICA as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA Client RSA Root CA 2021	1BE7ABE30686B16348AFD1C61B6866A0EA7F4821E67D5E8AF937CF8011BC750D	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

Table 7: Root-CA 4 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
CN=HARICA Client Authentication RSA,O=Hellenic Academic and Research Institutions CA,C=GR	858D7018873D31678AA155D071B3E0F2E09025169DD7938ECE98CAB81034A81D	[Technically-constrained non-Email Protection CA]
CN=HARICA S/MIME RSA,O=Hellenic Academic and Research Institutions CA,C=GR	B13EC301E7BFE1DDB9C5BFC071DC29C55E82EE933273A23134946FBDFD3ACE63	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=ACER Client Authentication RSA 4,O=Agency for the Cooperation of Energy Regulators,L=Ljubljana,C=SI	560F35BBA2B2232BEF7B749A0F35C5BB7C2848B530EB6172D81813C3707C5453	[Technically-constrained non-Email Protection CA]
CN=GEANT S/MIME RSA 1,O=Hellenic Academic and Research Institutions CA,C=GR	149C1FAC7DB7AF8868897D18529E6798DA20C0456439802B4CC8223FA1E476B3	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

Table 8: Sub-CA's issued by the Root-CA 4 or its Sub-CA's in scope of the audit

Root 5: HARICA Client ECC Root CA 2021

<p>Standards considered:</p>	<p>European Standards:</p> <ul style="list-style-type: none"> • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"> • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 1.7 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"> • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)
------------------------------	---

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

- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.9, as of 2025-03-14
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.8, dated 2024-07-17
- [\[CP/CPS\]](#) Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.7, as of 2023-07-17

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

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA Client ECC Root CA 2021	8DD4B5373CB0DE36769C12339280D82746B3AA6CD426E797A31BABE4279CF00B	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

Table 9: Root-CA 5 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
CN=HARICA Client Authentication ECC,O=Hellenic Academic and Research Institutions CA,C=GR	0F4BE73B561A822B273E8C5E65D118D78170A5B52FC7E5D047E4231138EC0A0B	[Technically-constrained non-Email Protection CA]
CN=HARICA S/MIME ECC,O=Hellenic Academic and Research Institutions CA,C=GR	E5CBD6659190C6188897D09E1AD62A4FB73CE11D8727A4476D3C579F0E1599F9	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6
CN=ACER Client Authentication ECC 1,O=Agency for the Cooperation of Energy Regulators,L=Ljubljana,C=SI	CA5EFC0F468C5751961FC76C0ACF38B9CF7B81D084F317B3AAA842CBA8FF9298	[Technically-constrained non-Email Protection CA]
CN=GEANT S/MIME ECC 1,O=Hellenic Academic and Research Institutions CA,C=GR	6EF2FEA64B86A61203FC7D53F2F212A8E3FB0E085934D60A5A88ABF46DCC2114A	ETSI EN 319 411-1: LCP, NCP, NCP+ amended by ETSI TS 119 411-6

Table 10: Sub-CA’s issued by the Root-CA 5 or its Sub-CA’s in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2025-06-27	Initial attestation

End of the audit attestation letter.