Audit Attestation for

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

Reference: No. 040321-01-KG

Thessaloniki, March 4, 2021

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 Audit Attestation Letter is registered under the unique identifier number "040321-01-KG" and consists of 10 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,

Karanikas Lazaros

Digitally signed by Karanikas Lazaros
Date: 2021.03.05 07:33:09 +02'00'

Lazaros Karanikas
Managing Director

Identification of the conformity assessment body (CAB):

QMSCERT

26th October Str., 90
546 27 Thessaloniki

Greece

Registered under n° 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)”.

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

[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

Identification of the audited Root-CA #1: HARICA TLS RSA Root CA 2021
Distinguished Name: C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA TLS RSA Root CA 2021
SHA-256 fingerprint: D95D0E8EDA79525BF9BEB11B14D2100D3294985F0C62D9FABD9CD999ECCB7B1D
SHA-256 SPKI: 693C9AA6B245B3B0261637750863EADB6C248A16E52D6F4BC90C86BBF32D7042
Applied policies ETSI EN 319 411-1 V1.2.2, DVCP ETSI EN 319 411-1 V1.2.2, IVCP ETSI EN 319 411-1 V1.2.2, OVCP ETSI EN 319 411-1 V1.2.2, EVCP ETSI EN 319 411-2 V2.2.2, QCP-w (Only with regard to key generation and key protection requirements)

Identification of the audited Root-CA #2: HARICA Qualified RSA Root CA 2021
Distinguished Name: C=GR, O=Greek Universities Network (GUnet), OU=Hellenic Academic and Research Institutions CA, organizationIdentifier=VATGR-099028220, CN=HARICA Qualified RSA Root CA 2021
SHA-256 fingerprint: DC73BCAA133E4AC2E72A3971A35DA701A30794F91A439110AE377CC097AA9EC5
SHA-256 SPKI: 64C7007A854EB3559C95BFB9DCA28AEBBDFCE725620AC1A547EA5792740C1920
Applied policies ETSI EN 319 411-1 V1.2.2, LCP ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, NCP+ ETSI EN 319 411-2 V2.2.2, QCP-n ETSI EN 319 411-2 V2.2.2, QCP-n-qscd ETSI EN 319 411-2 V2.2.2, QCP-l ETSI EN 319 411-2 V2.2.2, QCP-l-qscd ETSI EN 319 411-2 V2.2.2, QCP-w (Only with regard to key generation and key protection requirements)

Identification of the audited Root-CA #3: 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
SHA-256 SPKI: FBBA25C5A7B01994D56400A6DB705D523951A20BDE5B9AA9B87980899F65A355
Applied policies ETSI EN 319 411-1 V1.2.2, LCP ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, NCP+ (Only with regard to key generation and key protection requirements)

Identification of the audited Root-CA #4: HARICA Code Signing RSA Root CA 2021
Distinguished Name: C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA Code Signing RSA Root CA 2021
SHA-256 fingerprint: C40EBDCD75A90E4B7496ABB23E789A48E33C03284F75D95130575AE6860AE13C
SHA-256 SPKI: 1CA1DF4A0B8227C42AC2861F2B6B105F547D64C25C446CBE5C0C3849FD100A75
Applied policies ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, NCP+ ETSI EN 319 411-1 V1.2.2, EVCP (Only with regard to key generation and key protection requirements)

Identification of the audited Root-CA #5: HARICA TLS ECC Root CA 2021
Distinguished Name: C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA TLS ECC Root CA 2021
SHA-256 fingerprint: 3F99CC474ACFCE4DFED58794665E478D1547739F2E780F1BB4CA9B133097D401
SHA-256 SPKI: FC784300EC8DF4D3D1BAD763835182918D52A9FF0238BDF695A1CD9BDB98321C
Applied policies ETSI EN 319 411-1 V1.2.2, DVCP ETSI EN 319 411-1 V1.2.2, IVCP ETSI EN 319 411-1 V1.2.2, OVCP ETSI EN 319 411-1 V1.2.2, EVCP ETSI EN 319 411-2 V2.2.2, QCP-w (Only with regard to key generation and key protection requirements)

Identification of the audited Root-CA #6: HARICA Qualified ECC Root CA 2021
Distinguished Name: C=GR, O=Greek Universities Network (GUnet), OU=Hellenic Academic and Research Institutions CA, organizationIdentifier=VATGR-099028220, CN=HARICA Qualified ECC Root CA 2021
SHA-256 fingerprint: AC1CC116B03545F6D3E62CE32043198F527AB9E6E4F19FCCAA1D2F50C6438B0C
SHA-256 SPKI: 01F1FFEDB6518D6BCEE0E70F8A2C1FEB9A3FF1CBAE51AA5AA6CA8C2F0923EAD1
Applied policies ETSI EN 319 411-1 V1.2.2, LCP ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, NCP+ ETSI EN 319 411-2 V2.2.2, QCP-n ETSI EN 319 411-2 V2.2.2, QCP-n-qscd ETSI EN 319 411-2 V2.2.2, QCP-l ETSI EN 319 411-2 V2.2.2, QCP-l-qscd ETSI EN 319 411-2 V2.2.2, QCP-w (Only with regard to key generation and key protection requirements)

Identification of the audited Root-CA #7: HARICA Client ECC Root CA 2021
Distinguished Name: C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA Client ECC Root CA 2021
SHA-256 fingerprint: 8DD4B5373CB0DE36769C12339280D82746B3AA6CD426E797A31BABE4279CF00B
SHA-256 SPKI: DE56FC3CB78EEE9566A75C3BAEF1B220E92428FBFC570EA6A81A30FD46DAB7B7
Applied policies ETSI EN 319 411-1 V1.2.2, LCP ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, NCP+ (Only with regard to key generation and key protection requirements)

Identification of the audited Root-CA #8: HARICA Code Signing ECC Root CA 2021
Distinguished Name: C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA Code Signing ECC Root CA 2021
SHA-256 fingerprint: 794E774638CE7B3CF05EBC8967CF47315316C351DC26387476E0C099C2ED47CC
SHA-256 SPKI: 45594B86FF7AB29B444DC10842207BBBC3D36A5A948166D50D9365CFE995B8AA
Applied policies ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, NCP+ ETSI EN 319 411-1 V1.2.2, EVCP (Only with regard to key generation and key protection requirements)

The audit was performed as a point in time audit of root keys and root certificates generation ceremony at the TSP's location in Thessaloniki, Greece. It took place on 2021-02-19. The audit was performed according to the European Standards "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 the CA Browser Forum Requirements "EV SSL Certificate Guidelines, version 1.7.4" and "Baseline Requirements, 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 audit was based on the following policy and practice statement documents of the TSP:

1. Certificate Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, version 4.3, 2020-02-18

This audit covers the generation of root keys and root certificates of the aforementioned Root-Cas. It also covers the generation of the private keys referenced in Table 1 (RSA-4096) and Table 2 (ECDSA-384) and serves as the "birth certificate" of these keys. No Sub-CAs were generated during the ceremony.

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

#	SPKI
1	B977D10C295403097332F20929BCE4059FF418ABDA22FE0B9B87DD49BADBDDCD
2	1CC1A1BC596361497D9B3787993D86776ED7E981E432EC819930A555AE03B22A
3	5D76349DD75A2F3E02F3821371B8E3F24581D7234531067576FFC6CE1225A8D7
4	BACF813498B0DB5EB0AF3F4405504F0BFA7F695BA39E444DE587300C0387FF3A
5	62B0B583BDC85084C93B565291C60329E12244F82F13838FA5FCCF6B0F9AF0DC
6	EF549D93D757301400B6AB6A5F05DEAA48433575B5EEA4FDE573FFD5DA7CA46E
7	CEDFEFD4E087C51F7392B53EB3F56057CE426F7E05A8527912C5066321F52F2F
8	78E4725F4DC792FC1DA1EB4EA809299B7B3439E3CA1E9DF129601B5597979D50
9	B71E1397754F61B35B885A5E6F21205ED5E3344964193CF87BA6154E4E4293BE
10	36D04B9B5E0FB7821E1066D8524DA0AB60B7C39E958D9863F3C3A9C05CAF9BC5
11	1731866EC576EAB9E6651320F2CCDC874F0C8AE5B11E4FD6ED0D87F0426396DD
12	F19DF33B326FBA2836072930D5360F26A93AB012173E63D3C36A08DF12E71543
13	25D6402234F4172806B498A165AB96D8722B1A48EBFE1ADDC378E09860BC8BED
14	C103014EA08590CDFCF49A0F923C9D20BC904BE91EA2245D031E1817B731F90E
15	3F23C28883F6D4B652C768A1079CFB2140FDBC215D81B1E2DD3036C3F89B8149
16	9ED3082EA04388466CB0C587A2E7F2A6D382FF949D7A45CD0A20D365BADEB460
17	8571A4825F4385F07AED28E272C586EFB119B93169888C28E5723E1D2285C266
18	96918F80A7D23511C31317040DC066B09718D256631F51253ED664459C369D74
19	7A833A1A47BE6F70F9682F040F343BE6E040A9B92C5DCB1AD5EADB8F66F5DA10
20	CB6A0E5125A5088FE4B2C402FA2A9BF472B69749E668BF5C56C2564E465671BC

Table 1: Private keys (RSA-4096) created by the CA for future use

#	SPKI
1	9B830E8CED5E3BEA89762FDA97961D5C42C69E9552F6566813BB622E66E44CFD
2	87EEE9381093B72605E70D621B8BF6C4F35D6A96B04B80500CE0B818BC1FE89E
3	2FFBDF07ED88603CA7C6A6AA02AA6294A4EE7C5240B0C7379AE89B406F91091A
4	26E7B048D2D0414D8A7D5F1A074414806F1EF89F0E86246C36176DB85C543E36
5	7E3102FFB6E2A667CA6E6F32E8078D377E8B215E9826C42577B98F842D17DD5D
6	5F6679F7AB166F4F9E8F504E489BD23F34F1AF3D21155B7BEA8B3AB670071241
7	26AA8180BA7CA69BFE324B1F7874CB9699404A635919CC846B711C92B32FB134
8	D1134793B9F81F54BDD3372A28AE92393986F26C03AA1EE8320674AEC060533B
9	6225D515EA439909486454CF43D373AF3B2056A32E7A5ECEE3A1027D458EF11C
10	64D58B74ACF8FD427D2E76B37BC2FFCD4E82246DF5B804F51FE0D5F2AB782FB4
11	28E114AAFB55ED9CFD87655BFDEDA38ECD61435EC6F4381B5DBD1D366AA6189B
12	039B0DE82EB1BC6589CC66360B292B7E205AEFA41F2AF3034099C71AFF4A1EF6
13	E17EBD784CE0D8492741CDA16B6A48C4DD7F5ED5F1ADF9CD70929519056C72A6
14	B64A7FC569676697C042F175692B70AEEDDCE87FF77C0073DDFF9679D770EFFA
15	37A2E398E263D102A69483975F56FC2DD07DFE4D6A6989BF52E329527167D7CF
16	E47D08472A9DF5C8FB43E201258A40EA367784C77B4958B68052B84EAD17B6CF
17	0033CEFE0493358FADA40EFA54DC3E340A47559539E922F043AA2A6EF36E701E

18	AA0EDF4D20396E4F455547FAF22457D8C384D1015EF017D9C9AC910392532009
19	11B37A97B7815A5D2B8F8F479496B34306D5DF70DAC0EA38D7BB6513CF6F0284
20	1484A6143C98B8E3836D1819AC4308DBC0E03F301655BF933A0F6258907CC519
21	2E15587812AC4B24183257FC164610AAB41B7596F6E3026DAE3A363B02BCC79E
22	E8C05AFD2893A3D6A6E0BAC14106D9C7206D597A816B831FA07F1EB17688F3A9
23	BE8429563777689AF7DD15E57DE841D7A16694D7E77C277FF11CDD7B3358DFE7
24	220BD69F185D482F11155955380477D6C972B14D2EF470EE6634A796EBC57E76
25	D628D5CB99F4DB36A727D3CBEABF6C293266668202C2CBA875643435CAFAE2DD
26	5F16A138CFCD7F853E6C33D870A6744AA0B924A50AF8BB277A8A82ADFBE79CFE
27	AFD92AEFFD592E58D79769227C2C5EA3B584AF4A554291C35D00B39BF7DCF870
28	1A49D65B2C3AEF509D65EFBDE78F881CAB1C69218FD037ACBA1CE0E97551F1B6
29	221963708B614F3DE8C1FED6636028535F95A1BF6AE38AFC1E7FC15E939AD4CD
30	28605771A33BA6219597EB57C461084CEC3A1C203C9963B65D015883515BDAE0
31	5E5D4EBBFB1538451C8F90A110A7B8CE90E311C136953C9F4837F155584C3D08
32	911EBC156B0ECD13303055A754B298E3044C6CF4136BC5AEB2DAAC2C9AD91C8C
33	ADE0570E75610C8DA5513FE23F807DA62638A25EEAF1592CC906E01005C73B5B
34	D63675A98F769D83D25989BEB8141200626E6D210139BF9A02910600783C1604
35	BEF5A0FE73DE9972D353752B3D011E79740CF9CCB4784FDE8FB0AE5F805F4F70
36	6CC32177CB5DF286B7B81B30BFF54D5119461481FBEFE0CCAA13748CBCC12E39
37	F346E55BFD607E7CBAA2150F7DE6A1000302969ADD89F0E9200C2814E4EBD24E
38	CFFA3C3E75928882718DD0A83C7DA1AD3AC1BB5DAF093AFDD9E3713FE108CA6D
39	02760C1B67B51C55ABD5A907B7D0811A8110E5A269B2C5F68D157AA9A22E8C8E
40	508B6FD4CF0A2A5DE9B7B94D27131849564A3F86E3A680BE535479A273AA005E
41	7CCEA2402D1DC0E382CD5D5571DF03F16B11D6DDFAD3EA3EDD04F9F0CFB353D7
42	8F14E8C55C35D054FEC8DFE3C1B259D68B4C37E48E36FEADCF3079306B54067A
43	65F35E861A03B8BA5EC218B876CB4376A37A702711EE73B5F3EF335AC88C5BE9
44	A442BB8A524B442C37951551FCC8AC6ECDAEFDD1C1EC2FBB435D76651FC5587B
45	B03ECAF375759AB196CC3C51C529BA4D38F7EEB40ABF7765BDED260A7EAB767C
46	5467F55A72A194C792E5092AEA5A7F0F03ABA3886680DDE17F3571A67997C101
47	78E3EF0CB57589A639889D04F4ADC49FEB6C92F869A8CCF63D88CC66315ED6E5
48	3B3BD29132BEB299F12C6EEB68E55B18642F34FFE912D82F6FBCE163545A11CE
49	92E5F585BDD1518CCC68A7BE3DA2FD17A554842BC0C3673286DB6F1ED7788D8C
50	4CDBE0A4A7BD9F365F32F59134C3FE40E82CFD9B45DD44F74462D921A3ECDB5C

Table 2: Private keys (ECDSA-384) created by the CA for future use

Modifications record

Version	Issuing Date	Changes
Version 1	2021-03-04	Initial attestation

End of the audit attestation letter.