Audit Attestation for

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

Reference: 171120-01-KD

Thessaloniki, November 17, 2020

To whom it may concern,

This is to confirm that QMSCERT has audited the key destruction of Private Keys associated with Intermediate CA Certificates of the GREEK UNIVERSITIES NETWORK (dba "GUNET"), owner of HELLENIC ACADEMIC & RESEARCH INSTITUTIONS CERTIFICATION AUTHORITY ("HARICA"), without findings. The list of keys and associated Intermediate CA Certificates within the scope of this evaluation can be found in Table 1.

This present Audit Attestation Letter is registered under the unique identifier number "171120-01-KD" and consists of 18 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: 2020.11.17 13:26:04 +02'00'

Lazaros Karanikas
Managing Director

Identification of the conformity assessment body (CAB):	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)".

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

Identification of the audited Root-CA:	Hellenic Academic and Research Institutions RootCA 2011	
	Distinguished Name	C=GR/O=Hellenic Academic and Research Institutions Cert. Authority/CN=Hellenic Academic and Research Institutions RootCA 2011
	SHA-256 fingerprint	BC104F15A48BE709DCA542A7E1D4B9DF6F054527E802EAA92D595444258AFE71
	Applied policies	ETSI EN 319 411-1: LCP, NCP, NCP+, DVCP, OVCP, IVCP; ETSI EN 319 411-2: QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd
	Technical constraints	nameConstraints Permitted: DNS:gr DNS:eu DNS:edu DNS:org DNS:net email:.gr

[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

		email:.eu email:.edu email:.org

Identification of the audited Root-CA:	Hellenic Academic and Research Institutions RootCA 2015	
	Distinguished Name	C=GR/L=Athens/O=Hellenic Academic and Research Institutions Cert. Authority/CN=Hellenic Academic and Research Institutions RootCA 2015
	SHA-256 fingerprint	A040929A02CE53B4ACF4F2FFC6981CE4496F755E6D45FE0B2A692BCD52523F36
	Applied policies	ETSI EN 319 411-1: LCP, NCP, NCP+, DVCP, OVCP, IVCP, EVCP; ETSI EN 319 411-2: QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, QCP-w, QCP-w-psd2; ETSI EN 319 421: BTSP
	Technical constraints	-

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
	Applied policies	ETSI EN 319 411-1: LCP, NCP, NCP+, DVCP, OVCP, IVCP, EVCP; ETSI EN 319 411-2: QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, QCP-w, QCP-w-psd2; ETSI EN 319 421: BTSP
	Technical constraints	-

The audit was performed as a point in time key destruction audit at the TSP's location in Thessaloniki, Greece. It took place on 2020-11-02, with additional audit tasks between 2020-11-03 and 2020-11-12. The audit was performed in accordance with the requirements of the European Standards ETSI EN 319 411-1 V1.2.2 (2018-04), ETSI EN 319 401 V2.2.1 (2018-04) and ETSI EN 319 403 V2.2.2 (2015-08) for the Trust Service Provider Conformity Assessment.

During the key destruction ceremony, we were able to witness and confirm the following actions of the TSP. The TSP:

- prepared and approved a detailed CA key destruction script, which covered the destruction of the keys associated with the Intermediate CA Certificates in scope, in all of its operational HSMs, the destruction of their backups in any backup device and the revocation of all non-revoked CA Certificates in scope,
- applied effective controls to provide reasonable assurance that the process was executed in conformity with the CA key destruction script,
- performed all procedures required by the CA key destruction script and verified the destruction of the key material,
- performed the process in a physically secured environment,
- performed the process using personnel in trusted roles under multiple person control and split knowledge,

in accordance with its CP/CPS v4.2 (2020-09-30).

Our evaluation consisted of the following actions:

1. Review of the **CA key destruction script** for conformance with the applicable requirements and industry standard practices;
2. Identification of all **CA key sets** in question, the cryptographic devices (HSMs and slots) and their physical locations;
3. Identification of all related **backup files** and Master Backup Key (MBK) devices, including storage devices and physical locations;
4. Identification of the **complete history** of the key sets in question and their media (traceability);
5. Witnessing of the **secure storage location access process** and examination of the relevant access records;
6. Witnessing of the **execution of the key destruction ceremony**; this includes the verification of executing the selected key destruction methods per copy (of each key set), the use of trusted roles personnel under dual control and the physical and operational security aspects of the ceremony;

7. Examination of the **key destruction tools/scripts**;
8. Verification of the **revocation of the Intermediate CAs** in scope;
9. Examination of the secure audit logs of **OCSP responder configurations** since the birth of the oldest of the keys associated with the Intermediate CA Certificates in scope, in order to confirm that OCSP responders were not configured to use any of the private keys associated with the Intermediate CAs in scope;
10. Verification of any compensating controls;
11. Other tasks as appropriate.

#	CA Subject Distinguished Name	SHA-256 fingerprints	CA Issuer Distinguished Name	Applied policies	EKU	Other technical constraints[2]
1	CN=Ecclesiastical Academy of Vella Client RSA SubCA R1,O=University Ecclesiastical Academy of Vella of Ioannina,L=Ioannina,C=GR	Certificate fingerprint: 978BCF39C3C3AACEFE1048FA0360283DC2EBFA5150024C5E378514D3E75E7295 SPKI fingerprint: D87BF38B2D04ABD232473D112060AAC198E927EB	CN=Hellenic Academic and Research Institutions RootCA 2011,O=Hellenic Academic and Research Institutions Cert. Authority,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n, QCP-l-qscd, QCP-l	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
2[3]	CN=Ecclesiastical Academy of Vella SSL RSA SubCA R1,O=University Ecclesiastical Academy of Vella of Ioannina,L=Ioannina,C=GR	Certificate fingerprint: 58E368EE4D615B888E11C552B2CB3B469F30AC4BF48D8B379B51009C082643EC SPKI fingerprint: 4CDA90C6E631F93F9ECEB4ECAE4776FD0ABB3BB5	CN=Hellenic Academic and Research Institutions RootCA 2011,O=Hellenic Academic and Research Institutions Cert. Authority,C=GR	ETSI EN 319 411-1: DVCP, OVCP	TLS Web Client Authentication, OCSP Signing, TLS Web Server Authentication	Name Constraints
3	CN=Greek Federation of Judicial Officers Client SubCA R1,O=Greek Federation of Judicial Officers,L=Athens,C=GR	Certificate fingerprint: 2D819AF397E289DC41709C4AAF6DA3B1904749C37A995860745803716D7D5690 SPKI fingerprint: 22991B8E0FD3EB63EC4B5A26C5E347A8992AD4F2	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-2: QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
4	CN=GRnet Client RSA SubCA R1,O=Greek	Certificate fingerprint: A1A04E4CFC56FD1917EB48	CN=Hellenic Academic and Research Institutions	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-	TLS Web Client Authentication,	Name Constraints

[2] Other technical restrictions to limit the scope of Certificate issuance (as per BR §7.1.5)
[3] Revoked on 2019-03-18 (before the previous audit period)

	Research and Technology Network,L=Athens,C=GR	1FC46629A2E46656756FA08E22487F54B64E1CA3E7 SPKI fingerprint: 4EEE9BEF783FB7C4AD062CB4DE0374413F5C3C62	RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	2: QCP-n-qscd, QCP-n, QCP-l-qscd, QCP-l	E-mail Protection, Document Signing, OCSP Signing	
5	CN=Aristotle University of Thessaloniki Client RSA SubCA R1,O=Aristotle University of Thessaloniki,L=Thessaloniki, C=GR	Certificate fingerprint: 663FDE94F8836A1FEBD83BE8310979312D65FF8C1B716394E68F41D82396C1F8 SPKI fingerprint: BE8E6B084739CED16CC75EEBA98E4C6143C71017	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n, QCP-l-qscd, QCP-l	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
6[4]	CN=HARICA Administration Client ECC SubCA R1,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	Certificate fingerprint: 7CB888EF740DCBFC0C20BDA44F2C2619F6D0D4598FB932D037DAF278077773A5 SPKI fingerprint: 70F2EDEF391CF0488CCD4D637F8B8E5B3AF14033	CN=Hellenic Academic and Research Institutions ECC RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
7	CN=HARICA Administration Client ECC SubCA R2,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	Certificate fingerprint: 7A52945F5902D53C0DB76A200EB9F85C7C424B23F939FFE140C5DBD0B1F2C7D8 SPKI fingerprint: 9881B5E529A3887E9D0FBA55FE10DA206F38961B	CN=Hellenic Academic and Research Institutions ECC RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

[4] Revoked on 2019-03-07 (before the previous audit period)

8	CN=Academy of Athens Client SubCA R2,O=Academy of Athens,L=Athens,C=GR	Certificate fingerprint: BE6863CB0D3BB57314EE4B627FB346E8CD20581DE17FE0782AFB438EF034AC0B SPKI fingerprint: 777790FBECBF1D7812BBFDAE403BD5504749C6A2	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
9	CN=Aristotle University of Thessaloniki Client RSA SubCA R2,O=Aristotle University of Thessaloniki,L=Thessaloniki, C=GR	Certificate fingerprint: 48395F71CC26F64274BD06C7EB1591F9D4EC62B64FA6C16531F3CB72C2469D82 SPKI fingerprint: 62357BF4B871F4BED880146BF5E0452CD79B7A27	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
10	CN=Ecclesiastical Academy of Vella Client RSA SubCA R2,O=University Ecclesiastical Academy of Vella of Ioannina,L=Ioannina,C=GR	77BBABD8E1C2AA51AFCE71D6AD940E219647B9320245C4BBBD6B31DD28E1F32C SPKI fingerprint: F08CB232BFC744064704FC0696750DCBCB9977ED	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
11	CN=GRnet Client RSA SubCA R2,O=Greek Research and Technology Network,L=Athens,C=GR	Certificate fingerprint: 1CC3F7B1368F476010DBB254B3970B859C94524C6B62EBCE946C8AE63939E68F SPKI fingerprint: F041BCE2D240DC98F3F423B53A7167ACC89DBCCC	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

12	CN=Greek Federation of Judicial Officers Client SubCA R2,O=Greek Federation of Judicial Officers,L=Athens,C=GR	Certificate fingerprint: 0EF3960A0811490F4D53E33FAFC41F5C94EEB1667A1A2CC96BF3F29D619CAF88 SPKI fingerprint: 6F0400FCD299F279539DCD939406C7D56BDDB9CC	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-2: QCP-n-qscd	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
13	CN=GRNET Client RSA SubCA R3,O=National Infrastructures for Research and Technology,L=Athens,C=GR	Certificate fingerprint: F808656236725B566F0721C518158A6756C96903CB71EB48DDDA8EDDFEA0F26C SPKI fingerprint: 58BAB1976BC9E8B13028E0D82B36B3CAC601FC33	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
14	CN=International Hellenic University Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	4E78271768494088ED1F9BB2712531AB5D138C6C59B46650D285B35858E67B13 SPKI fingerprint: CBA77738A70A8B3FEA51A9EA7E94B5AFD4304926	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
15	CN=University of Ioannina Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 42A21F37285804F2E736075CB54874368CF0E2110088B3F138412EEC88590954 SPKI fingerprint: 980C3258F62B9A9E2ED79DB71C5AC164220062CA	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

16	CN=University of Patras Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 46716EBF6A22AEA1DF1F97E62A5EF7095127CE4550B6242EBA6907AFC5C482CF SPKI fingerprint: 280B99AA2FEE750517B60FD89EF96B26F4E80CBC	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
17	CN=National Technical University of Athens Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 887D7F1DEB7F0712C85AFABF50CADF89BF02EB13E552CBF52D7B5DF3F21DB0DA SPKI fingerprint: 52E00BB41B91047E4A7C5843A51E9B68F7CEB71D	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
18	CN=University of the Aegean Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 55B80DEF607F88E31C584067D09D43344D94117BAF648365847B1CE5B67677C9 SPKI fingerprint: CD0523FEFB603CE27E81E948FC9A43C12712115F	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
19	CN=Ionian University Client RSA SubCA R2,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek	Certificate fingerprint: FC3A98938E2ED3BD36E0D41F18517649322906B2E6B33690891325AAECD19644	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

	Universities Network (GUnet),C=GR	SPKI fingerprint: E2AC23AC14B4D5CDABC156DBA1C1CE17EEA1380D				
20	CN=Aristotle University of Thessaloniki Client RSA SubCA R3,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 523575047371BBA88263E5AB5DED8F6B0695C5D2A192A6DD11406C476BA3C72F SPKI fingerprint: 8B173D39872CFAF8833F318E363465653B5E2FEA	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
21	CN=Greek Federation of Judicial Officers Client RSA SubCA R3,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 2A508A5FE6173C4E8F0126694A1A6A71D9000451FA31DB033B8705890441ECC5 SPKI fingerprint: ADF074B79F551C342A2C516D47A0A1DD8B3C7B12	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-2: QCP-n-qscd	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
22	CN=Academy of Athens Client RSA SubCA R3,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: FD2F33248F39645646879802 35A5F0BCB3AB562E47F404F742E53342C5375280 SPKI fingerprint: 5352753E1C29BE1F06CC7C27CFF9EBA3AC4FA38F	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

23	CN=GRNET Client RSA SubCA R4,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 538A45AAF9003D4D3988BBFCF9F859B325CE5F775DC0601205058517F9BC15E5 SPKI fingerprint: 945AA34F46A0F129E93D27E61436627CBB41B74C	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
24	CN=Ecclesiastical Academy of Vella of Ioannina Client RSA SubCA R3,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: E74AD44B0D56EEBE39BB185C52AB9BEFE4F75899B6A81416E9103D5C29BF27FB SPKI fingerprint: EE3E364052E28BA4852202E0DB3803B379697C61	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
25	CN=Athens University of Economics and Business Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: E77AC02DB6EAA0E9A6B573A99870C6DF4DBDB8339DDA3BC40786F70E2BD7F7F6 SPKI fingerprint: 2C52F3DFA7B7E37AABEB93ED4FD8A8FC3F4CF63D	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
26	CN=CEDEFOP Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek	Certificate fingerprint: 1E953E15123A95E47044BFAF06B1974FB9976B84F4371EBD77F8AD81EFD05C00	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, Document	Name Constraints

	Universities Network (GUnet),C=GR	SPKI fingerprint: 63AADE3228756297C30BEB80FF84580B41813028			Signing, OCSP Signing	
27	CN=Democritus University of Thrace Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: E57BBF5079F98293B4142F348972E68E351E52B90373F05F46F09CCB30AF5BF0 SPKI fingerprint: 62A8E94D35DD90CE75ABA13D6815CC98D05F2B0C	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
28	CN=Greek Universities Network Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: BD4420C592A6F7F252AE898124E002F1B9CFE1F2538864D56B34A7B4DFB31FC8 SPKI fingerprint: 00E4496D610AD2E587ED0DAD32E287DD9F6FEFCA	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
29	CN=HEAL-LINK Hellenic Academic Libraries Link Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 084ECA70A9B40E4E1563E35776B716E410A972BB27ED51C248C48D3242FA8DAF SPKI fingerprint: BBCBF1C12A6F19BA56A35890CA29866A340603A1	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
30	CN=Harokopio University Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions	Certificate fingerprint: 6EC8D3551BD0454B0CC4B9DB876366AE08764C5FCF15B00F9411BDE30D5336AE	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection,	Name Constraints

	CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	SPKI fingerprint: 10E6F375A92AC54B11968B6968B448EE1C24487B	Institutions Cert. Authority,L=Athens,C=GR		Document Signing, OCSP Signing	
31	CN=Inst. of Accelerating Sys and Applications Client RSA SubCA R2,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: A8E352DB0C8E27BAE583D015146E8B79DEE091D5638F583A0C442F3BF55DEEB3 SPKI fingerprint: 9F061DB50ADEBC0D0C26CB40758CD909FD4D42C5	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
32	CN=Panteion Univ. of Social and Political Sciences Client SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 2D1B244FACEAFAD94755B5E99AABF7AC91C599DA73BFA461EEEBAFB4B969B5C9 SPKI fingerprint: 3B4E927739CB0ED64324C09906096B2E9B0013B1	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
33	CN=Greek School Network Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: EADC80F7DF630560CC1B353F68EA660159CE966E22D404588780787C0476D0E4 SPKI fingerprint: D6CF5BB9E29A6F5DF0EA11C6BC18123E0D0E26DC	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

34	CN=Technical University of Crete Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 22E5E6DB5CAE428EDA96AED0564E2B9770ECA2CC025158E37A9DDEEDE31F45E5 SPKI fingerprint: 2A894660B60AC4E402E8659E4E99E6469CA31449	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
35	CN=University of Piraeus Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: BC489C6DC2BDE253F586DA34134D6640B8B583A312089CE10933C4BC03FC5F33 SPKI fingerprint: 7A6EFAE67FBB9603DE9E3B1B4E42F04574399A28	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
36	CN=National and Kapodistrian Univ. of Athens Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: F3D916D1B73201F049EDA7E597FE0A5CCD5711A6958FBC0B7A6F7FA64F7AFE47 SPKI fingerprint: 20DDBDE7F481A74A742A2FE879BCFE0B776EDD6B	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
37	CN=University of Crete Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek	Certificate fingerprint: 87AAD978A5FE2EE941E4068F9963EA29BDAA58878D2412249A82CD22F8126D82	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

	Universities Network (GUnet),C=GR	SPKI fingerprint: 8E4BAC241E661F15F63C3625EA018DA02EFD8389				
38	CN=University of Macedonia Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 444CEFEDD83F6315C5EC86B2F1CD63B1DBF2387CFA2BEB0FB400153F2AF9408F SPKI fingerprint: A5AA25B64CD2B655C61CDEDC2782CB385222B675	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
39	CN=University of the Peloponnese Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: EA4793E2EB814D43261F8068AEFDE783B837E7C021AC19C8E9B08551F2D6C83F SPKI fingerprint: ED95A6E17280F63608458923653CF21772DB182A	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints
40	CN=University of Western Macedonia Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 0CB6684F601C416F992A89409914A32A0C2099716875F5F78EC0C46B1B57099C SPKI fingerprint: C0860CAB88E80D704C127C515C5B295C4693A781	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

41[5]	CN=University of West Attica Client RSA SubCA R1,OU=Hellenic Academic and Research Institutions CA,organizationIdentifier=VATGR-099028220,O=Greek Universities Network (GUnet),C=GR	Certificate fingerprint: 7D35BF04C857282B422E851EA8A622B75D2ECCBAB65D5BA62598C1DA4A11D502 SPKI fingerprint: 7CAA1D9ED61E717F2D14809217C1EA59FA071D22	CN=Hellenic Academic and Research Institutions RootCA 2015,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR	ETSI EN 319 411-1: NCP, NCP+; ETSI EN 319 411-2: QCP-n-qscd, QCP-n	TLS Web Client Authentication, E-mail Protection, Document Signing, OCSP Signing	Name Constraints

Table 1: Sub-CA's for which key destruction has been audited

[5] Issued after the previous audit period (on 2020-05-20)

Modifications record

Version	Issuing Date	Changes
Version 1	2020-11-17	Initial attestation

End of the audit attestation letter.