

QMSCERT® CERTIFICATE

QMSCERT, an accredited provider of third-party system certification organization for ISO/IEC 27001 information security management systems and acting in accordance with the requirements of ISO 17021 for registrars attests that:

HELLENIC ACADEMIC & RESEARCH INSTITUTIONS CERTIFICATION AUTHORITY - HARICA

NETWORK OPERATIONS CENTER,
NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS
operator site address:
IT CENTER, ARISTOTLE UNIVERSITY OF THESSALONIKI

with a scope of:

Provision of Certificate Authority Services

*& with documented ETSI Certification Policy
Revision No: 3.4 Issue Date: April 20th, 2016*

has established a management system that is in conformance with the ETSI Standards

TS 101 456 V1.4.3, TS 102 042 V2.4.1

Policy Requirements

LCP, NCP, NCP+, QCP, QCP+, DVCP, OVCP

June 8th, 2018

Certification Period Ending

June 9th, 2015

Initial Certification Date

June 9th, 2015

Certification Date



For the QMSCERT Board

This certification is subject to Annual Surveillance Audits. The certification is valid (for three years) only if it is followed by the annual surveillance audits approval.

For information concerning the validity of the certificate, you can visit the site www.qmscert.com



QMSCERT® N. 270415/5414 Rev.1

This certificate is accompanied by Annex A (Audit Report) which is renewed every year

QMSCERT® 26th OCTOBER 90 Str. - 54627 - THESSALONIKI - HELLAS

QMSCERT®

Annex A (Surveillance Audit Report) to Certificate No: 270415/5414 Rev.1

Organization's Name: Hellenic Academic & Research Institutions Certification Authority (HARICA)

Issue No: 2, Issue Date: July 8th, 2016

APPLICABLE ETSI CERTIFICATION POLICY:

CP/CPS VERSION 3.4, APRIL 20TH, 2016

OID: 1.3.6.1.4.1.26513.1.0.3.4

Background

The HARICA Public Key Infrastructure (PKI) is a trusted third entity which certifies the identities of network users and servers affiliated with Academic and Research Institutions of the Hellenic Republic. The HARICA PKI is a consortium between equal members that are Academic Institutions, Research Institutions and the Greek Research and Technology Network (GRNET) which is the Greek National Research and Educational Network (NREN) and began during the VNOC2 project (funded by GRNET through the Operational Program "Information Society"). HARICA is currently funded by the Greek Universities Network (GUNET). This service is available for the members of the Hellenic Academic and Research Institutions. HARICA has been certified for both ETSI TS 101 456 and ETSI TS 102 042 standards since 2011, and seeks to extend further to provide Qualified Certificates. It has passed through full Re-Certification Audit on April 2015; current report refers to the Surveillance Audit which took place on April 2016 as planned.

Assessment Context

Q-CERT Ltd (distinctive title QMSCERT), as the body carrying out the audit, is accredited by the official Hellenic Accreditation System (ESYD) as conforming to ISO/IEC 17021, and also accredited in line with ISO 27006 to carry out ISO 27001 audits.

Accreditation Certificate: No.110-3, refer to <http://esyd.gr/portal/p/esyd/en/showOrgInfo.jsp?id=17715>
ESYD is a full member and signatory to the multilateral agreement (MLA) of both International Accreditation Forum (IAF) and the European Cooperation for Accreditation (EA), and in fact one of its founding members. QMSCERT is committed to providing and maintaining certification services that are discrete, non-discriminatory, ethical, professional, and focused to legal and other implied or expressed requirements for the benefit of all interested and relevant parties.

Specifications Context

The examination was conducted in accordance with the following European Standards:

- ETSI TS 102 042 V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates", Version 2.4.1, 2013-02, European Telecommunications Standards Institute
- ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing qualified certificates"
- ETSI TS 119 403 V.2.1.1 (2014-11): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers"

and, where applicable, has considered all CA/Browser Forum Requirements, in particular:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v. 1.3.4 of the CA/Browser Forum adopted by Ballot 162 on March 15, 2016.

QMSCERT®

Annex A (Surveillance Audit Report) to Certificate No: 270415/5414 Rev.1

Organization's Name: Hellenic Academic & Research Institutions Certification Authority (HARICA)

Issue No: 2, Issue Date: July 8th, 2016

in order to meet the policy requirements for:

- LCP, NCP, NCP+, QCP, QCP+, DVCP and OVCP reference policies

Moreover, all applicable European and National laws and regulations have been considered, in particular:

- Presidential Decree 150/2001 "Adaptation to directive 99/93/EE of European Parliament and Council with regard to the Community frame for electronic signatures"
- FEK 603/B/16-5-2002 "Regulation on the Provision of Electronic Signature Certification Services"

Audit Procedure

Audit Team has been selected on the basis of proficiency and competency in order to prepare and carry out the audit, report its results and submit its recommendation for Technical Review and Certification Decision, according to the established internal procedures of the Certification Body.

Lead Auditor:

- Nikolaos Soumelidis, QS (ISO 9001:2008) & ISMS (ISO/IEC 27001) Lead Auditor

Technical Review / Certification Decision:

- Lazaros Karanikas, Management Systems Lead Auditor

Surveillance audit was conducted in two phases (according to full audit rules):

- Documentation review phase, which verified the conformance of documented statements, policies and procedures against the Specifications Context, and reviewed all actions taken by the organization in order to improve the Management System, in accordance with the Re-Certification audit remarks.
- On-site implementation review phase, which verified that all the above improvement initiatives and all audited policies and procedures (documented or not) were properly implemented into the actual operations of the organization in conformance with the Specifications Context.

Audit took place on sampling basis, under the inherent limitations of the system controls themselves and only in the scope and purpose of the Specifications Context. Under no circumstances should it replace a potential in-depth technical audit (e.g. vulnerabilities or penetration audit), which might be considered as one of the risk treatment options. Its purpose was to verify the conformance of the CA's management system against the requirements of the aforementioned standards.

Internal reports for both stages were documented by the audit team, and its recommendation was submitted for technical review and certification decision, according to the Certification Body's standard procedures, also audited and approved by the national Accreditation Body.

The conditions to conduct the audit were fully met prior and during the audit.

Audit Results

During technical review, all audit results and internal reports were reviewed, and the CA was found to be **fully compliant** with the provisions of the Specifications Context. **Improvement remarks** have also been submitted by the Certification Body for review by the CA, in order to assist its continuous efforts for improvement, in line with the PDCA model. This Certificate has been issued by the Certification Body in order to officially confirm this positive assessment.

QMSCERT®

Annex A (Surveillance Audit Report) to Certificate No: 270415/5414 Rev.1

Organization's Name: Hellenic Academic & Research Institutions Certification Authority (HARICA)

Issue No: 2, Issue Date: July 8th, 2016


In particular, the independent audit confirmed compliance as follows:

- A Certification Policy and Certification Practices Statement (CP/CPS) for the Hellenic Academic and Research Institutions Public Key Infrastructure has been issued and is available online at <http://www.harica.gr/documents/CPS-EN.pdf>
- CP/CPS has been approved by Senior Management of the CA and contains all necessary provisions as specified in the applicable standards and requirements, including those required for the extension to Qualified Certificates.
- The CP/CPS document is an integral part of the management system documentation which has been established by the CA; system also includes internal procedures, guides, forms and records which form a complete framework for the management of the security and quality of the provided trust services.
- Documentation, including CP/CPS document, is monitored and reviewed regularly by CA's authorized personnel in order to meet updated requirements, changes in the context or business processes or the organization, or technical developments.
- The implementation of the management system is also monitored and reviewed both in terms of daily operations by CA's authorized personnel, but also through Internal Audits and Management Review.
- Risk Management process is used in order for the CA to assess threads and weaknesses, measure risks and form adequate action plans to mitigate risks.
- All relevant roles and responsibilities have been identified and assignments have been made to qualified CA personnel, in order to form a competent administration team. All CA's administration personnel have been found as qualified for their background, training, experience and professional diligence.
- Independent audit confirmed the adequacy and proper implementation of all necessary controls to comply with CA practice requirements (Ch. 7). These include controls for all Key and Certificate management life cycle (7.1-2) processes, namely key generation, storage, backup, recovery, distribution, subject registration, certificate generation, revocation, dissemination of certificates and terms and conditions to subscribers and relying parties.
- Proper controls have been implemented to ensure clear and undeniable acceptance of the terms and conditions by subscribers prior to dissemination or usage.
- CA has removed previous restrictions (i.e. "Academic and Educational purposes, and only under the .gr, .edu, .eu and .org domains") for the use of its Certificates; this is an extension planned and prepared already prior to the previous audit, and includes improvement actions taken in the interim.
- CA does not undertake any liabilities, including financial, civil or other responsibilities, except for cases where there is evidence of fraudulent intent or serious negligence by its operators.
- CP / CPS has been updated in order to meet the specifications context for Cross-Signing services; in order to provide these, CA shall plan and develop the processes needed for service realization.
- In order to provide its services to new markets, CA shall seek any opportunities to further enhance its capacity, including but not limited to liability coverage, human & infrastructure resource improvements.

Next Audit

According to scheduling rules of ISO 17021 standard, in order for this Certificate to remain valid until its expiration date, a 2nd Surveillance Audit should take place between nineteen (19) and twentyfour (24) months period since 27/04/2015 (on-site audit Stage II completion date); thus, between 27/11/2016 and 26/4/2017.




For QMSCERT