**Deventum IT Excellence**
**a:** L. Nikis 3, 54624, Thessaloniki
**t:** +30 2310 239119
**e:** info@deventum.com

**Title**

# INDEPENDENT AUDIT REPORT BASED ON THE REQUIREMENTS OF ETSI TS 101 456

**Customer**

**HARICA**
**( www.harica.gr )**

**To**

**WHOM IT MAY CONCERN**

**Date**

**18 March 2011**

**Deventum IT Excellence**
**a:** L. Nikis 3, 54624, Thessaloniki
**t:** +30 2310 239119
**e:** info@deventum.com

**To whom it may concern,**

This is an official document to declare the following facts upon request by HARICA. (Hellenic Academic Research Institutions Certification Authority).

The HARICA Public Key Infrastructure (PKI) is a trusted third entity ( http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/EsignProviders.html ) 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 currently is funded by GUnet SA, (http://www.gunet.gr), a nonprofit civil company that was founded in 2000. GUnet has its central office in Athens and its members are all the Higher Education and Academic Institutions (20 Universities and 16 TEI). The aims of the company are determined by the broadband network needs and objectives of the Greek academic community in the framework of Information Society aiming at servicing research and education. Due to the nature of GUnet and as far it concerns the well-being status of HARICA we can safely assume that the later will be able to maintain its functionality and proper funding through time.

1. Deventum has been selected by HARICA as the auditor for the electronic certificate services provided by HARICA.
2. HARICA has been audited by our company under the standards and technical specifications based on ETSI TS 101 456.
3. HARICA has disclosed its key and certificate life cycle management business and information privacy practices in its Certification Practice Statement http://www.harica.gr/documents/CPS-EN.php and provided such services in accordance with its disclosed practices and,
4. Maintained effective controls to ensure that:
   i) Subscriber information is properly authenticated.
   ii) The integrity of keys and certificates it manages are established and protected thought their life cycles
   iii) Subscriber and relying party information are restricted to authorized qualified personnel.
   iv) The continuity of key and certificate life cycle management operations is maintained.
   v) The use of trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them
   vi) CA systems development maintenance and operations are properly authorized and performed to maintain CA systems integrity.

Based on the ETSI TS 101 456, Electronic Signatures and Infrastructures Policy requirements for Certification Authorities.

Based on our audit and source code audit of the website, scripts and procedural documents we specifically can conclude on the following results. HARICA personnel was found qualified and able to perform proper changes to ensure the security of the website ( http://www.harica.gr ) as well prepared on all issues described by the ETSI TS 101 456 requirements.

Our findings, based on the requirements of the ETSI TS 101 456, as described on the following Audit Report.

**On demonstrating the reliability necessary for providing certification services**

a) Policy and practices

The CA's policy is fully described on the "Certification Policy and Certification Practices Statement" document and published accordingly [1]. The documentation covers the practices and procedures used to address all the requirements, identifies the obligations of all external organizations supporting CA services including policies and practices.

Documentation [1] as well as terms and conditions and the Memorandum of Understanding [2] can be publicly found on the web available to subscribers and relying parties on the website of the CA, http://www.harica.gr .

The management body and authority statuses responsible for approving the certification practice statement are well documented and presented on the MoU documentation [2].

b) On business continuity management and incident handling

HARICA presented the documentation on the business continuity plan addressing disaster recovery plan as well the compromise or suspected compromise of CA's private singing key as disaster. The document [3] can be acquired upon request from the CA.

c) CA Termination

Procedures on the CA's termination can be found on the MoU document [2] for the relying parties and on the CP/CPS documentation for the CA available at section 5 paragraph 8 of the CP/CPS documentation [1].

d) Organizational structure

Under the MoU documentation [2] HARICA's legal body is described as well as the management structure and organizational structure. Detailed information covering the personnel experience, knowledge and background can be disclosure under request and given a need to know basis from the CA's archives.

**On ensuring the operation of a prompt and secure directory and a secure and immediate revocation service**

a) Certificate dissemination

HARICA as described on the CPS documentation [1] section 4 paragraph 2, Certificate Application Processing, ensures that certificates are made available as necessary to the subscribers, subjects and relying parties. More on the certificate lifecycle is publicly available under the chapter 4 of the CPS documentation [1].

b) Certificate revocation and suspension

The auditor can confirm that based on the source code audit and procedural audit of the CA, the CPS policy describing that certificates are revoked in a timely manner based on authorized and validated certificate requests as described on [1] section 4 paragraph 9 “Certificate Revocation and Suspension”.

c) System Access Management

Under our audit procedures we were able to verify the continuous monitoring and alarm facilities as they are described on section 5 of document [1], “Administrative, Technical and Operational Controls”.

**Ensuring that the date and time when a certificate is issued or revoked can be determined precisely**

a) Precise time

As defined in the CA’s CPS documentation [1] section 6 paragraph 8, we were able to verify that proper NTP servers were used and timestamps are logged on every action performed by the CA systems.

**Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued**

Even though HARICA is not defined as a qualified certificate authority and the certificates are not meant to be qualified the following procedures are performed to verify the identity of the subject issued a certificate in order to meet the technical specifications for qualified CAs.

a) Subject registration

Based on the CPS document [1] section 3, paragraph 2 Initial identity validation and Authentication of Individual person identity on section 3 paragraph 2 subsection 3 of the same document: the certificates of individuals that are issued by the HARICA PKI must be checked for identification. There are two classes of user certificates. Class A includes certificates whose private key is generated and resides in a secure cryptographic device (eToken or smartcard) and are issued under the presence of authorized personnel of the RA. Class B includes certificates whose private key has been generated using some software (software certificate store). It is clear there is a secure identification of the recipient with her/his physical presence and an acceptable official document proving his identity at both classes of certificates.

The Registration Authority relies on the control of identity performed by the institutions the subscriber belongs to and uses authentication ways of user identities that are available in the institutions in order to check the identity. The collaborating institutions are compelled to have certified the identity of a user by means of an official document that bears the photograph of the beneficiary (eg. police identity, passport, driving license, student identity card) and which is considered reliable by the familiar institution. Alternatively, the RA of HARICA can execute the above process of applicant identification.

In case the familiar institution of the user, according to its policy, has already performed a procedure of physical identity verification in the past (e.g. for the provision of a user account or e-mail address) there is no need to repeat the procedure but a typical confirmation through the officially certified e-mail address of the user is sufficient.

HARICA central RA uses two methods for e-mail ownership and control verification:

1) The first method uses simple e-mail verification. The user enters the e-mail address at the initial certificate request form and a verification e-mail is sent to the user with a link to a unique web page. After following this link, an e-mail is sent to the institution's network operation center mail administrator that requires an approval based on the full name entered by the user and the user's email. This approval requires the identification of the user with his/her physical presence and an

acceptable official document. If this procedure took place before (e.g. for the creation of an e-mail account) then there is no reason to be repeated.

2) The second method uses an LDAP server. The user enters the personal e-mail address at the initial certificate request form and the corresponding password. This information is verified against the institution's LDAP server. If the verification is successful, the RA queries the real name of the user and creates the certificate request. In order for a user to be listed in the Institutional Directory server, the institution must have verified the user with his/her physical presence and an acceptable official photo-id document.

Certificates of Class A are recommended to include an extra organizational unit (OU) in the subject field with the value 'Class A – Private Key created and stored in hardware CSP. Certificates of Class B are recommended to include an extra organizational unit (OU) in the subject field with the value 'Class B – Private Key created and stored in software CSP [4].

b) Certificate renewal, rekey and update

To ensure that requests renewal, rekey and update requests are coming from a subject who has already previously registered and properly authorized, the procedures on the CA's CPS [1] section 4 paragraph 6 Certificate Renewal, section 4 paragraph 7 Certificate Re-keying and section 4 paragraph 8 Certificate Modification are described and followed as such.

**On employing personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards**

We found the followings:

a) Security management and
b) Personnel security

Administrative and management procedures are applied which are adequate and correspond to recognized standards. Specifically, we found that HARICA describes at the CPS document [1], section 5 paragraph 3 subsection 1, "Personnel handling roles of Certification Authorities and Registration Authorities must have experience in digital certificates and Public Key Infrastructure issues. They must also have experience in managing sensitive personal data and classified information in general."

c) Operations management

We found that the CA operates with responsibility on the following topics as they are described on the ETSI TS 101 456,

- operational procedures and responsibilities;
- secure systems planning and acceptance;
- protection from malicious software;
- housekeeping;
- network management;
- active monitoring of audit journals, event analysis and follow-up;
- media handling and security;
- data and software exchange.

And documented on CP/CPS documentation [1] section 5 paragraph 1 under "Physical security and access controls".

**Use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the processes supported by them**

As we mentioned above the CA systems are limited to individuals with the proper authorization access. Especially according to ETSI TS 101 456 policy,

a) System management access

A full network layout and the levels of security implementation by the means of firewalling, process accounting, internal and external IDS monitoring and availability monitors were demonstrated by the CA authorized personnel, as described on [1] section 6 paragraph 7 “Network Security Controls”.

b) Trustworthy Systems Deployment and Maintenance

As described on the CPS and given the level of access that we as auditors could have we were able to verify the use of trustworthy systems and products that are protected by modification. Further on the risk analysis and business continuity plan [3] provided documentation on the critical services.

c) Certification authority key generation

We were able to verify that the generation of the Certification Authority key meets the requirements identified in FIPS PUB 140-2 level 3 and the physical environment is secured during the process. The detailed description of the device is described on [1] section 6 paragraph 1 subsection 1.

d) Certification authority key storage, backup and recovery

As we could observe the CA follows the CPS documentation [1], section 6 paragraph 2 subsection 4, “The private key must be kept at a backup copy. The backup copy of the private key must be encrypted and the procedures referenced at section 5 paragraph 1 subsection 6 must be followed. Access to the backup copy is allowed only by authorized personnel.”

e) CA provided subject key management services

During our code audit review we found the CA compliant with the ETSI TS 101 456 policy and acting accordingly to the CPS documentation under [1], section 6 paragraph 2 “Private key protection and Cryptographic Module Engineering controls”.

**Take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data**

During the audit procedure and based on [5] specifications the CA is acting accordingly to the CPS documentation on the following topics:

a) Certification authority key storage, backup and recovery

The CA private keys remain confidential and maintain their integrity, as defined on [1] section 6 under “Technical security controls”.

b) Certification authority public key distribution

Based on [1], CAs provide mechanisms for the secure digital delivery of all certificates. Each digital certificate contains the public key when it is requested by interested entities. Interested entities may send a request by email. The CA can also send a certificate via snail-mail in a magnetic media device, which contains the public key. All certificates of each CA are published through a secure web site, whose identity is certified by a different trusted third party. Detailed description provided on section 6 paragraph 1 subsection 4 of [1]

c) CA provided subject key management services

**Deventum IT Excellence**
**a:** L. Nikis 3, 54624, Thessaloniki
**t:** +30 2310 239119
**e:** info@deventum.com

As defined on the CPS documentation [1] we can verify that the use of SHA1 algorithm is used for the generation of the subject keys. Detailed description of the algorithm provided on section 7 paragraph 1 subsection 3 of [1].

d) Subject registration

As described above on "Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued." [above]

e) Certificate renewal, rekey and update

As described above on "Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued." [above]

f) Certificate generation

The CA complies with the standard format for non-qualified certificates and follows the documentation of the [1], as described on section 6 "Technical security controls" and section 7 "Certificate, CRL and OCSP Profiles".

**Maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive [6], in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance**

As described on the CPS documentation [1] section 9 paragraph 14 "Governing law" and section 9 paragraph 8 "Limitation of liability",

CPS [1] section 9 paragraph 14:

HARICA is focused on serving the Hellenic Academic and Research Community. Each certificate issued, clearly states in the Certificate Policy Notice field that "*This certificate is subject to Greek laws and our CPS. This Certificate must only be used for academic, research or educational purposes*". No financial transactions will take place with HARICA PKI unless otherwise specified in a sub-CA with a separate CP/CPS. The operation of the HARICA PKI as well as the interpretation of the CP/CPS is subject to the Academic ethics and in the national Greek Legislation. Particularly as far as the Presidential Decree 150/2001 «Adaptation to directive 99/93/EE of European Parliament and Council with regard to the Community frame for electronic signatures» is concerned, the certificates that are published they **ARE NOT** generally considered as "Qualified Certificates", although the CAs and the issued certificates **MEET** the technical requirements for "Qualified Certificates".

Under specific conditions and treaties, the certificates that are published can be used as 'qualified' in closed teams of entities, as for example in certain administrative service of Academic Institutions.

These procedures must be described on a separate Certification Policy/Certificate Practice Statement (CP/CPS) document that correspond to that particular subordinate Certification Authority, taking account and meeting all the requirements (including the liability issues) described in the Presidential Decree 150/2001. As stated in section 1 paragraph 3 subsection 3, these procedures must not conflict with any condition of the present document.

Basic conditions for this "qualification" and accordingly the "qualification" of a relative produced digital signature as equivalent to a handwritten signature include:

a) The use of "secure environment for the creation of digital signatures" in the subscriber's side (e.g. smart card exclusively in which the private key is created, stored and used) and

b) The official approval of each responsible body (eg. senate or governing board of an Institution). [1]

CPS [1]: section 9 paragraph 8

*HARICA PKI cannot be held liable for any problems or damages that may arise from its services or from wrongful, negligent or improper use of the issued certificates. HARICA does not undertake any financial, civil or other responsibilities*. Using HARICA and its certification services requires that users unconditionally accept the terms and services of this CP/CPS and that HARICA is not liable and does not undertake any financial, civil or other responsibilities, except for cases where there is evidence of fraudulent intent or serious negligence by its operators. [1]

**Record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically**

Based on [5] we have the following requirements,

a) Recording of Information Concerning Qualified Certificates.

Since HARICA is not issuing qualified certificates the CA is not required by law to keep recordings of information. Still, HARICA retains information that can be used when needed as described on [1] section 5 paragraph 4 subsection 3, section 9 paragraph 4 subsection 5.

b) CA termination

As described on the CPS documentation [1] section 5 paragraph 8, “Certification Authority or Registration Authority termination”,

“Upon its termination, each CA informs its subscribers, revokes all certificates issued, updates the relevant CRL and revokes its own certificate. Finally, it informs the security officers and publishes for the end of its operation. The log files of the CA and RA are kept for two (2) years to be available for any lawful control. This period may be modified depending on developments of the relevant legislation.” [1]

**Not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services**

We were able during the audit to verify the following:

a) CA provided subject key management services

As described above on “Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued.” [above]

**Before entering into a contractual relationship with a person seeking a certificate to support his electronic signature, inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate**

ETSI documentation [5] requirements on,

a) Subject registration

As described above on “Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued.” [above]

b) Dissemination of Terms and Conditions

The CA provided us during the audit with the MoU documentation as well as the CPS where terms and conditions for subscribers and relying parties are described. During the request and at the process of

obtaining a certificate, the subject must accept the terms and conditions. Furthermore the documentation can be publicly accessed on the following addresses:

i) http://www.harica.gr/documents/MoU.en.pdf
ii) http://www.harica.gr/documents/CPS-EN.html

**Use trustworthy systems to store certificates in a verifiable form so that:**

- **only authorized persons can make entries and changes;**
- **information can be checked for authenticity;**
- **certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained; and**
- **any technical changes compromising these security requirements are apparent to the operator.**

As we covered earlier during our audit review,

a) Certification authority public key distribution

As we covered above on “Take measures against forgery of certificates and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data.” [above]

b) Certificate dissemination

As we covered above “On ensuring the operation of a prompt and secure directory and a secure and immediate revocation service” [above]

c) Certificate revocation and suspension

As covered above, “On ensuring the operation of a prompt and secure directory and a secure and immediate revocation service” [above]

d) System Access Management

As covered above, “On ensuring the operation of a prompt and secure directory and a secure and immediate revocation service” [above]

e) Trustworthy Systems Deployment and Maintenance

As covered above, “Use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the processes supported by them.” [above]

**Conclusion**

Based on our audit on the procedures and policy as well as on the code audit performed over the web site, scripts and functions of the CA we found HARICA to be compliant with the ETSI TS 101 456 technical specifications, as non-qualified Certificate Authority, issuing non-qualified certifications.

Although it meets the technical requirements for qualified CAs, HARICA chose not to be qualified because its purpose is used only for academic and educational purposes. No financial transactions will take place with certificates issued by HARICA unless otherwise specified in a sub-CA with a separate CP/CPS

This Audit Report is based on the requirements and guidelines specifically described on ETSI TS 101 456 and does not include any professional opinion whatsoever as regards to the quality of the services rendered by HARICA, nor of their suitability for the specific objectives of any subscriber, beyond the ETSI TS 101 456 criteria for Certification Authorities that are covered herein.

**Deventum IT Excellence**
**a:** L. Nikis 3, 54624, Thessaloniki
**t:** +30 2310 239119
**e:** info@deventum.com

Due to limitations inherent to the control systems themselves, there may be undetected errors or instances of fraud. Moreover, the reaching of any conclusions in periods subsequent to the date of our report, based on our statements, is subject to the risk that there may be:

1) Changes in the source code, controls or the established system,
2) Changes in processing requirements,
3) Changes brought about by the passage of time itself, or
4) That the degree of compliance for policies or procedures may alter the validity of our conclusions.

**Deventum IT Excellence**
**a:** L. Nikis 3, 54624, Thessaloniki
**t:** +30 2310 239119
**e:** info@deventum.com

**INDEX**

1. Certification Policy and Certification Practices Statement for the Hellenic Academic and Research Institutions Public Key Infrastructure, http://www.harica.gr/documents/CPS-EN.pdf
2. Memorandum of Understanding for the operation of the HARICA Public Key Infrastructure, http://www.harica.gr/documents/MoU.en.pdf
3. HARICA procedures and regulations, PKI Disaster Recovery Plan by Dimitris Zacharopoulos.
4. Authentication of individual person identity http://www.harica.gr/documents/CPS-EN.pdf, section 3 paragraph 2 subsection 3.
5. ETSI TS 101 456 technical specification "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
6. The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.

**Deventum IT Excellence**
**a:** L. Nikis 3, 54624, Thessaloniki
**t:** +30 2310 239119
**e:** info@deventum.com

**This Audit Report has been prepared for Deventum by:**

- **Nicolas Krassas, CISSP Certification Number: 94337**
- **Dimitrios Stergiou, CISA Certification Number: 0973230, CISSP Certification Number: 305086, CISM Certification Number: 09549256**
- **Dimitrios Papapetros, CISA Certification Number: 1189862**

**Nicolas Krassas, CISSP**

**18 March 2011**