Aristotle University of Thessaloniki

Information Technology Center

Public Key Infrastructure

Certification Policy and Certificate Practice Statement

Version 4.0 (Jun 5th 2015)

Document Manager:
Dimitris Zacharopoulos

Working Group:
Dimitris Zacharopoulos
Fotis Loukos
Apostolos Papagiannakis
Ioannis Feneris

Table of Contents

1 Introduction

This Certification Policy and Certification Practice Statement (CP/CPS) describes the set of rules followed by Certification Authorities that participate in the Public Key Infrastructure (PKI) of the Aristotle University of Thessaloniki (AUTH). The AUTH Public Key Infrastructure was established in 2001 by AUTH Network Operations Center (NOC) with the creation of an independent ROOT Certification Authority. AUTH-NOC took the initiative and proposed the creation of a wider-scale Public Key Infrastructure for the Hellenic Academic and Research community. This initiative was mainly supported by the University of Aegean and the Greek Research and Technology Network (GRNET) and in 2006 the Hellenic Academic & Research Institutions Certification Authority (HARICA) was established (http://www.harica.gr). The Aristotle University of Thessaloniki trying to widen the Certification Authorities web of trust, migrated from a stand-alone Certification Authority, to a Certification Authority under the HARICA Root Certification. HARICA is currently funded by the Greek Universities Network (GUNET – http://www.gunet.gr). In 2013, AUTH-NOC was merged along with other central University ICT Centers to form the "Information Technology (IT) Center", a new University Directorate, which is now responsible for the Public Key Infrastructure of Aristotle University of Thessaloniki.

1.1 Overview

This Certification Policy and Certification Practice Statement, describes the set of rules and procedures concerning digital certificates within the AUTH Public Key Infrastructure.

The terms and conditions specified in this CP/CPS abide to the relevant terms and conditions of the HARICA Root CA, as specified in the HARICA CP/CPS latest version, which can be found at http://www.harica.gr/documents/CPS.php.

The AUTH Certification Authorities issue user certificates, Network Device Certificates (e.g. servers, routers etc.) and Subordinate Certification Authority Certificates. All certificates contain a reference to this document. Certificate owners and relying parties, must be aware of this policy document and must comply with its statements.

1.2 Document Name and Identification

This document is called "Certification Policy and Certification Practice Statement of AUTH Public Key Infrastructure" and constitutes the documentation and regulatory frame of AUTH Public Key Infrastructure and Certification Authority. In abbreviation, it must be referred as "AUTH CP-CPS".

The Certification Policy defines, documents and makes known to all interested entities (e.g. members of academic community, collaborators, subscribers, third-party entities that rely on the validity of the provided services, other organizations, Institutions and Authorities) the terms and the operational practices that are applied or govern the Certification Services that AUTH PKI provides.

The structure of this document is based on the standard IETF RFC-3647 with the minimum necessary changes in order to reflect the particular needs of the Academic community. This document also adopts guidelines and specs from the CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v1.2.5".

The globally unique Identification Number (OID) of this document is: 1.3.6.1.4.1.**7709.2.0.4.0** where:

1.3.6.1.4.1.**7709**	Identification Number (OID) of AUTH, registered to IANA (www.iana.org)
2	Certification Services Provision
0	Certification Practice Statement
4.0	First and Second digit of the version number of the Certification Practice Statement

1.3 PKI Participants

The entities that use digital certificates issued by AUTH Public Key Infrastructure constitute the community governed by this Certification Policy and Certification Practice Statement.

1.3.1 Certification Authorities

Certification Authorities (CA) are the entities of the Public Key Infrastructure responsible for issuing certificates. Every Certification Authority utilizes one or more Registration Authorities (RAs). RAs provide the means of communication between the users and the corresponding Certification Authority.

The hierarchy of the Certification Services Provider was initially constituted by the following entities:

1. Central Certification Authority (AUTH-CENTRAL-CA) which issues digital certificates exclusively for Subordinate Certification Authorities that operate within Aristotle University of Thessaloniki. As an exception, it is allowed to issue a certificate for the OCSP responder according to RFC2560 and draft-cooper-pkix-rfc2560bis-00.txt (see Figure 7 of the draft: “Designated OCSP Responder and CA with Two Keys Certified by Root CA”).
   The validity period of AUTH-CENTRAL-CA certificate is eight (8) years.
2. Subordinate Certification Authorities that operate in administrative, academic units or other legal entities of AUTH, which comply with and fully adopt this Certification Policy and Certification Practice Statement. The maximum validity period of the certificates of the Subordinate Certification Authorities is four (4) years.

1.3.2 Registration Authorities

Registration Authorities (RA) are entities responsible for identity validation of all applicants before the issuance of the certificate. They transfer the requests to the particular Certification Authority in a secure manner. AUTH IT Center is the central Registration Authority of PKI and applies strict procedures for users’ authentication, at least as strict as the ones specified in the HARICA CP/CPS.

1.3.3 Subscribers

PKI subscribers are entities who request and successfully acquire a digital certificate signed by an AUTH Certification Authority. Subscribers can be entities (persons that have a contractual, academic relationship or affiliation with AUTH and devices operated by AUTH).

The rules and procedures specified in the HARICA CP/CPS, such as the subscription of roles, apply.

1.3.4 Relying Parties

The Relying Parties are all the entities that trust the provided certification services of the AUTH PKI and the HARICA PKI, as specified in the HARICA CP/CPS.

1.3.5 Other Participants

Not specified.

1.4 Certificate Usage

The certificates can be used by the members of the wider academic and research community and other parties. All appropriate and forbidden certificate usages can be found in the HARICA CP/CPS.

1.5 Policy Administration

1.5.1 Policy Making Organization

ca-admin@it.auth.gr
Information Technology (IT) Center of AUTH
Faculty of Sciences
1st floor of the Biology Department Building
AUTH campus
54124 Thessaloniki,
Greece

1.5.2 Contact Persons

pki@auth.gr

Dimitris Zacharopoulos [jimmy@it.auth.gr]
Tel: 2310 998483
Fax: 2310 999100

Yannis Salmatzidis [jsal@it.auth.gr]
Tel: 2310 998398
Fax: 2310 999100

Information Technology Center of AUTH
Faculty of Sciences
1st floor of the Biology Department Building
University campus of AUTH
54124 Thessaloniki
Greece

1.5.3 Policy Enforcement Persons

pki@auth.gr

Dimitris Zacharopoulos [jimmy@it.auth.gr]
Tel: 2310 998483
Fax: 2310 998492

Yannis Salmatzidis [jsal@it.auth.gr]

Tel: 2310 998398
Fax: 2310 999100

Information Technology (IT) Center of AUTH
Faculty of Sciences
1st floor of the Biology Department Building
University campus of AUTH
54124 Thessaloniki
Greece

1.5.4 CPS Approval Procedures

The CP/CPS is approved by the Computing and Communication Networks Committee of Aristotle University of Thessaloniki.

1.6 Definitions and Acronyms

The definitions and acronyms of the HARICA CP/CPS, as stated in section 1.6 of the HARICA CP/CPS, apply.

2 Publication and Repository Responsibilities

2.1 Repositories

The AUTH PKI has a central data repository where policy documents, certificates of Certification Authorities and certificates of subscribers/devices are published. Distributed repositories may exist for each subordinate Certification Authority/Registration Authority that participates in the PKI.

2.2 Disclosure of Certification Authority

The AUTH CA maintains a repository accessible through the Internet in which it publishes the Digital Certificate of the Central Certification Authority (type X.509.v3), the Digital Certificates that are issued according to the Certification Practice Statement, the current CRL and other documents regarding its operation (e.g. Cooperation agreements).

The CA performs all the necessary actions for the uninterrupted - as possible - availability of its repository.

The AUTH PKI repository address is http://www.pki.auth.gr/rep_dyn.

Moreover, the storage and search of certificates and CRLs is possible using the directory service of AUTH.

2.3 Frequency of Publication

The provisions of section 2.3 of the HARICA CP/CPS apply.

2.4 Access Control

The access control measures specified in section 2.4 of the HARICA CP/CPS apply.

3 Identification and Authentication

3.1 Naming

The naming specified in section 3.1 of the HARICA CP/CPS applies.

3.1.1 Type of Names

The provisions specified in section 3.1.1 of the HARICA CP/CPS apply.

Additionally, the attribute “O=Aristotle University of Thessaloniki” must be included in all user, device, service and code signing certificates.

3.1.2 Obligation for meaningful names

The provisions specified in section 3.1.2 of the HARICA CP/CPS apply.

3.1.3 Anonymity or pseudonymity of subscribers

The provisions specified in section 3.1.3 of the HARICA CP/CPS apply.

3.1.4 Rules for interpreting various name forms

The provisions specified in section 3.1.4 of the HARICA CP/CPS apply.

Additionally, the attribute “O=Aristotle University of Thessaloniki, C=GR” must be included in the Distinguished Name of all user, device, service and code signing certificates.

3.1.5 Uniqueness of names

The provisions specified in section 3.1.5 of the HARICA CP/CPS apply.

3.1.6 Resolution Process regarding disputes about naming property rights and the role of trademarks

The regulatory body for matters concerning disputes about naming property rights at AUTH-PKI is the AUTH Rector’s Office, after the recommendation of the Computing and Communication Networks Committee of Aristotle University of Thessaloniki.

3.2 Initial identity validation

The methods for the proof of possession of the private key and the authentication of the organization identity specified in section 3.2 of the HARICA CP/CPS apply, where Institution is the Aristotle University of Thessaloniki.

Furthermore, the method supported by the Aristotle University of Thessaloniki for the e-mail ownership and control verification is the SAML-based Single Sign On (SSO) Architecture, as specified in the HARICA CP/CPS.

Issuance of SSL/TLS certificates is allowed only for domains belonging to the Aristotle University of Thessaloniki. In order for a user to apply for an SSL/TLS device certificate he must own a user certificate which proves his identity. Then a verification e-mail is sent to the Aristotle University of Thessaloniki’s IT Center’s designated administrators who verify the validity of the FQDN of the certificate request. They also check that the person who applied for the certificate is the rightful owner/administrator of the FQDN according to the Aristotle University of Thessaloniki database of users / servers. No other method of FQDN verification is allowed.

3.3 Identification and Authentication for re-key requests

Re-key requests are handled according to section 3.3 of the HARICA CP/CPS.

3.4 Identification and authentication for revocation requests

Revocation requests are handled according to section 3.4 of the HARICA CP/CPS.

4 Certificate Life-cycle Operational Requirements

4.1 Certificate Application

An application for certificate issuance can be submitted by a subscriber according to the HARICA CP/CPS from the web page of the Registration Authority, http://www.pki.auth.gr/ or through the RA of her/his AUTH School or Faculty.

4.2 Certificate Application Processing

Certificate applications are processed according to the procedure defined in section 4.2 of the HARICA CP/CPS.

4.3 Certificate Issuance

Certificates are issued according to the procedure defined in section 4.3 of the HARICA CP/CPS.

4.4 Certificate Acceptance

Certificate acceptance is conducted according to the procedure defined in section 4.4 of the HARICA CP/CPS.

4.5 Key Pair and Certificate Usage

The usage of the certificates issued by the Aristotle University of Thessaloniki PKI and the related key pairs are defined in section 4.5 of the HARICA CP/CPS.

4.6 Certificate Renewal

The certificate renewal is handled according to the procedure defined in section 4.6 of the HARICA CP/CPS.

4.7 Certificate Re-keying

The certificate re-keying is handled according to the procedure defined in section 4.7 of the HARICA CP/CPS.

4.8 Certificate Modification

The provisions of section 4.8 of the HARICA CP/CPS apply.

4.9 Certificate Revocation and Suspension

Certificate Revocation and Suspension is handled according to section 4.9 of the HARICA CP/CPS.

The URLs that may be used by the software vendors for User Agent Validation are the following:

- https://www.pki.auth.gr which provides a “valid” certificate
- https://revoked.pki.auth.gr which provides a “revoked” certificate
- https://expired.pki.auth.gr which provides an “expired” certificate.

4.10 Certificate status services

The certificate status services defined in section 4.10 of the HARICA CP/CPS are used.

4.11 End of subscription

The provisions of section 4.11 of the HARICA CP/CPS apply.

4.12 Key Escrow and Recovery

Key escrow and recovery is handled according to section 4.12 of the HARICA CP/CPS.

5 Administrative, Technical and Operational Controls

5.1 Physical security and access controls

The Central Certification Authority of AUTH is currently located at the Information Technology (IT) Center of the Aristotle University of Thessaloniki. Other subordinate Certification Authorities may be located inside and outside AUTH IT Center.

The physical security and access controls defined in section 5.1 of the HARICA CP/CPS apply.

5.2 Procedural controls

The procedural controls defined in section 5.2 of the HARICA CP/CPS apply.

5.3 Personnel controls

The personnel controls defined in section 5.3 of the HARICA CP/CPS apply.

5.4 Audit logging procedures

The audit logging procedures defined in section 5.4 of the HARICA CP/CPS apply.

5.5 Records archival

The records archival procedures defined in section 5.5 of the HARICA CP/CPS apply.

5.6 Key changeover

The key changeover procedures defined in section 5.6 of the HARICA CP/CPS apply.

5.7 Compromise and disaster recovery

The compromise and disaster recovery procedures defined in section 5.7 of the HARICA CP/CPS apply.

5.8 Certification Authority or Registration Authority termination

The Certification Authority or Registration Authority termination procedures defined in section 5.8 of the HARICA CP/CPS apply.

6 Technical security controls

6.1 Key pair generation and installation

The provisions and controls defined in section 6.1 of the HARICA CP/CPS apply.

6.2 Private key protection and Cryptographic Module Engineering Controls

The provisions and controls defined in section 6.2 of the HARICA CP/CPS apply.

6.3 Other aspects of key pair management

The provisions and controls defined in section 6.3 of the HARICA CP/CPS apply.

6.4 Activation data

The provisions and controls defined in section 6.4 of the HARICA CP/CPS apply.

6.5 Computer security controls

The provisions and controls defined in section 6.5 of the HARICA CP/CPS apply.

6.6 Life cycle technical controls

The provisions and controls defined in section 6.6 of the HARICA CP/CPS apply.

6.7 Network security controls

The provisions and controls defined in section 6.7 of the HARICA CP/CPS apply.

6.8 Time-stamping

The provisions and controls defined in section 6.8 of the HARICA CP/CPS apply.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate profile

The Certificate profile defined in section 7.1 of the HARICA CP/CPS is used.

7.1.1 Name constraints

AUTH Central CA applies name constrains on all CAs according to RFC 5280. This extension is marked as "non-critical" and limits all certificates to the "auth.gr" domain.

It is also feasible to issue server certificates for educational or research activities at the other domains via a special purpose subCA operated by the HARICA central infrastructure.

7.1.2 Certificate policy object identifier

The OID (Object Identifier) of the certificate policy 1.3.6.1.4.1.**7709.2.0.4.0**, which complies with the CP/CPS of AUTH PKI, version 4.0, is included in the subscriber certificates.

7.2 CRL Profile

The CRL profile defined in section 7.2 of the HARICA CP/CPS is used.

7.3 OCSP Profile

The OCSP profile defined in section 7.3 of the HARICA CP/CPS is used.

8 Compliance Audit and Other Assessments

The Aristotle University of Thessaloniki PKI meets the specifications of ETSI TS 101 456 *"Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates"*, ETSI TS 102 042 standard *"Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"* and the Precedential Decree 150/2001. An external CP/CPS compliance audit is required on a yearly basis.

The Aristotle University of Thessaloniki PKI has also included guidelines and procedures from the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document, produced by the CA/Browser Forum (www.cabforum.org).

A compliance audit may be conducted on demand by interested parties, provided there is appropriate permission by the Aristotle University of Thessaloniki IT Center and as long as the interested parties cover the audit expenses.

9 Other Business and Legal Matters

9.1 Fees

No dues are paid for the provided services. Furthermore, the provisions of section 9.1 of the HARICA CP/CPS apply.

9.2 Financial responsibility

The Aristotle University of Thessaloniki PKI cannot undertake or pay damages for potential liability, unless specified otherwise in the current CP/CPS. Furthermore, the provisions of section 9.2 of the HARICA CP/CPS apply.

9.3 Confidentiality of business information

The Aristotle University of Thessaloniki PKI does not handle commercial type of information. Furthermore, the provisions of section 9.3 of the HARICA CP/CPS apply.

9.4 Privacy of personal information

The provisions of section 9.4 of the HARICA CP/CPS apply.

The process of the disclosure of classified and personal information to the judicial authority, if there is an official court order according to the privacy and data protection applicable law, is carried out through the Aristotle University of Thessaloniki Rector's office.

9.5 Intellectual property rights

The provisions of section 9.5 of the HARICA CP/CPS apply.

9.6 Representations and warranties

The provisions of section 9.6 of the HARICA CP/CPS apply.

9.7 Disclaimers of warranties

The provisions of section 9.7 of the HARICA CP/CPS apply.

9.8 Limitations of liability

The provisions of section 9.8 of the HARICA CP/CPS apply.

9.9 Indemnities

The provisions of section 9.9 of the HARICA CP/CPS apply.

9.10 Term and termination

The provisions of section 9.10 of the HARICA CP/CPS apply.

9.11 Individual notices and communications with participants

The provisions of section 9.11 of the HARICA CP/CPS apply.

9.12 Amendments

The provisions of section 9.12 of the HARICA CP/CPS apply.

9.13 Dispute resolution provisions

Differences or disputes that result from the interpretation of this Certificate Policy/Certification Practice Statement and the operation of the Certification Authority will be solved according to the Academic deontology and the Greek Law. In the case of disputes it is Greek courts that are competent and the venue is Thessaloniki Greece.

9.14 Governing law

The provisions of section 9.14 of the HARICA CP/CPS apply.

9.15 Compliance with applicable law

The provisions of section 9.15 of the HARICA CP/CPS apply.

9.16 Miscellaneous Provisions

The provisions of section 9.16 of the HARICA CP/CPS apply.

10 ANNEX A (AUTH CENTRAL CA)

```
=== BEGIN AUTH CENTRAL CA R4 ===

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:dd:87:ae:1f:4b:b6:6d
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic
and Research Institutions RootCA 2011
        Validity
            Not Before: Jan  9 12:44:39 2014 GMT
            Not After : Jan  7 12:44:39 2022 GMT
        Subject: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Aristotle
University of Thessaloniki Central CA R4
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9b:f8:cf:29:92:61:8e:66:39:52:e5:e1:7f:0f:
                    e1:41:39:90:72:62:03:29:ff:77:0f:cd:f3:c9:e0:
                    72:5d:2f:05:5a:13:73:bb:15:0d:77:cd:96:ff:3d:
                    9d:0d:c2:80:cf:df:b5:7b:f4:85:38:e1:35:f7:81:
                    0f:44:af:2c:36:a8:98:d9:62:8b:76:a6:15:58:a6:
                    ed:8a:21:aa:36:45:a5:04:30:a7:f5:fc:3f:a7:df:
                    a4:ed:94:4f:1c:08:56:3a:9c:57:d9:d3:0d:b6:4e:
                    43:4a:40:34:6e:22:24:cf:d3:25:68:5b:03:6a:ea:
                    02:a3:42:a1:9f:09:43:aa:31:56:ed:8a:f4:00:b9:
                    d2:82:6a:28:82:d1:d2:44:d0:15:ff:a7:27:ba:fb:
                    19:99:94:7c:cf:fd:e8:f4:81:b0:80:86:84:e1:22:
                    95:e4:5d:90:33:86:35:f9:1a:e6:dd:4a:e9:af:0a:
```

```
                    09:5f:93:f6:da:4d:7f:2b:0a:0a:f2:a9:6a:fd:13:
                    7d:06:90:ad:38:b7:89:85:a8:98:93:ee:2a:ff:6c:
                    cc:46:0b:0a:53:3b:3c:52:01:4d:9d:91:5c:4a:4e:
                    3a:f0:d7:77:c2:1b:3d:93:aa:66:e9:b4:28:96:58:
                    28:bb:51:04:fe:de:df:ea:a3:0f:c9:cd:2a:a8:f1:
                    8b:23
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                F5:93:17:4A:1D:73:B6:7F:7F:20:B2:A5:14:94:57:72:19:33:36:D2
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crlv1.harica.gr/HaricaRootCA2011/crlv1.der.crl

            X509v3 Authority Key Identifier:
                keyid:A6:91:42:FD:13:61:4A:23:9E:08:A4:29:E5:D8:13:04:23:EE:41:25

            Authority Information Access:
                OCSP - URI:http://ocsp.harica.gr
                CA Issuers - URI:http://www.harica.gr/certs/HaricaRootCA2011.pem

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.26513.1.0.2.7
                  CPS: http://www.harica.gr/documents/CPS.php
                  User Notice:
                    Organization: Hellenic Academic and Research Institutions Certification Authority
                    Number: 1
                    Explicit Text: This certificate is subject to Greek laws and our CPS. This Certificate
must only be used for academic, research or educational purposes.

            X509v3 Name Constraints:
                Permitted:
                  DNS:auth.gr
                  email:auth.gr
                  email:.auth.gr

    Signature Algorithm: sha1WithRSAEncryption
        57:50:a8:d3:f3:3e:b6:fd:2e:db:0a:02:80:f6:86:47:d6:ec:
        7a:75:49:e7:3d:fd:86:cd:89:eb:85:05:40:73:7b:75:9e:31:
        96:62:44:3e:46:74:37:09:87:fd:b2:e3:2d:33:7b:13:c5:ff:
        e3:fc:1d:98:df:4d:79:3c:78:63:67:29:24:1b:ab:70:8a:39:
        c7:1e:24:e8:a4:3e:33:48:03:d0:ba:d5:0f:ab:61:c1:1d:2a:
        4f:ee:ee:d0:5d:24:49:ce:4a:04:b6:a7:6e:da:ab:95:06:1d:
        f1:6a:23:70:18:d0:ec:4e:e1:92:9c:21:5d:2c:ee:ef:d5:fb:
        96:9f:cf:52:b9:95:91:11:0e:9d:f5:d5:f1:05:bf:63:79:72:
        98:77:37:e1:cf:b1:e5:d1:1d:e6:07:29:9f:bf:3c:67:2e:24:
        df:7f:97:2c:ec:f4:19:e7:c3:22:7c:28:52:74:87:b8:40:83:
        8b:cb:e0:1b:65:de:7a:29:40:b6:8e:da:f9:ab:a8:62:eb:81:
```

```
        ba:02:7b:d0:26:98:cb:23:c9:14:94:62:d1:8b:96:06:3d:e8:
        5c:a4:5d:b5:89:52:53:9f:87:98:34:ff:67:69:6e:f6:4e:5d:
        ce:80:66:e4:46:59:bf:7f:33:28:97:7f:12:db:3d:08:4b:00:
        28:95:0c:a4
```

=== END AUTH CENTRAL CA R4 ===

=== BEGIN AUTH CENTRAL CA R5 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:dd:87:ae:1f:4b:b6:79
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic
and Research Institutions RootCA 2011
        Validity
            Not Before: May  5 13:35:54 2015 GMT
            Not After : May  3 13:35:54 2023 GMT
        Subject: C=GR, O=Aristotle University of Thessaloniki, CN=Aristotle University of Thessaloniki
Central CA R5
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e3:bc:e8:96:27:d8:2f:a2:0e:89:1c:ac:71:7c:
                    2f:c2:7d:a8:a5:29:2a:72:a4:a0:67:eb:63:3c:33:
                    74:a3:cc:a5:89:f1:5d:3c:80:f1:ea:b0:60:bc:8e:
                    99:cd:90:2e:70:f8:8a:45:08:90:dc:cd:37:8e:4d:
                    50:03:98:96:5a:ca:b3:f7:7b:34:dc:25:0b:f6:87:
                    b6:8f:25:9e:a5:ad:ea:61:f8:6c:d7:49:ce:65:a6:
                    f1:a4:6f:cf:ad:73:40:cb:a2:0c:98:35:1c:ad:42:
                    ab:9c:47:b6:7c:0c:08:59:07:ed:eb:4b:6f:33:14:
                    b3:a4:e1:8c:3f:f1:2a:1d:e3:54:45:53:9b:1c:bf:
                    87:74:6d:3c:e4:b6:3b:ec:01:c1:94:91:69:57:63:
                    6a:e9:e1:03:f9:66:04:8d:68:7e:91:1e:b2:cb:6d:
                    28:d2:a2:dd:aa:1d:52:18:42:8c:c3:59:33:c9:1b:
                    43:22:2b:24:8b:cb:60:fb:9e:32:ec:5a:ab:80:19:
                    bb:97:a4:d9:eb:88:9c:7b:23:b2:31:ea:fa:cd:bf:
                    1c:9e:ee:35:7a:33:ba:9c:cd:0d:6c:27:c4:13:3f:
                    ad:2e:ec:59:03:82:31:6d:c9:d0:37:59:37:2d:19:
                    a9:46:a7:45:95:30:86:da:f2:6f:c4:cf:f2:98:d7:
                    72:29
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                74:91:84:CD:8F:9B:C5:C8:FB:3E:A3:74:F2:4E:74:BB:F9:9A:EE:46
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crlv1.harica.gr/HaricaRootCA2011/crlv1.der.crl

            X509v3 Authority Key Identifier:
                keyid:A6:91:42:FD:13:61:4A:23:9E:08:A4:29:E5:D8:13:04:23:EE:41:25

            Authority Information Access:
                OCSP - URI:http://ocsp.harica.gr
                CA Issuers - URI:http://www.harica.gr/certs/HaricaRootCA2011.crt
```

```
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.7709.2.0.3.6
                  CPS: http://www.pki.auth.gr/documents/CPS.php
                  User Notice:
                    Organization: Hellenic Academic and Research Institutions Certification Authority
                    Number: 1
                    Explicit Text: This certificate is subject to Greek laws and our CPS. This Certificate
must only be used for academic, research or educational purposes.

            X509v3 Name Constraints:
                Permitted:
                  DNS:auth.gr
                  email:auth.gr
                  email:.auth.gr

    Signature Algorithm: sha256WithRSAEncryption
        a6:4b:c3:e8:7a:ef:1b:cc:51:7a:65:ee:94:3e:70:7e:72:07:
        b6:a4:94:87:a7:dc:48:9c:6f:ca:f0:19:95:46:5f:ae:c9:46:
        8c:18:76:27:37:49:21:e1:8f:74:1f:55:4a:ea:63:e3:d0:e0:
        3c:14:2a:23:e1:9b:c3:c2:af:4a:e5:05:2f:fe:b9:8d:f2:35:
        84:fe:ff:e8:a9:4a:35:64:bb:97:fd:fc:06:be:e0:59:7f:93:
        23:f9:54:ad:11:0d:c3:13:25:17:1a:40:ea:1a:ff:14:6e:f7:
        83:2c:bc:20:f5:bc:cc:e5:b4:e7:ec:6e:b6:82:b9:8c:ae:9e:
        bf:19:c3:50:5f:ad:c8:23:13:77:2e:3e:9d:7d:5d:67:b5:a8:
        89:1e:a3:be:a3:b6:e4:fe:6f:90:1c:07:22:be:a3:90:ed:ee:
        44:cb:ae:cf:0c:d4:10:8c:7d:dd:35:12:a0:0d:d9:68:0e:5b:
        67:05:44:5a:72:d2:77:0d:e1:6e:c1:c3:85:6f:6e:7d:04:a6:
        1b:2c:33:22:bd:58:fb:38:c5:24:3e:75:4e:40:03:6a:a7:01:
        16:bc:f8:c3:39:44:43:58:db:77:ba:ad:f8:f8:e9:c1:e3:d2:
        58:41:4c:ed:b1:fd:f8:b2:6a:20:aa:1e:ae:ad:03:f9:3b:38:
        12:60:dd:f1
=== END AUTH CENTRAL CA R5 ===
```

11 ANNEX B (AUTH PKI Certificate Profiles)

The profiles defined in Annex B of the HARICA CP/CPS are used.