Network Operations Center
Aristotle University of Thessaloniki

Public Key Infrastructure at Aristotle University of Thessaloniki

Certification Policy and Certification Practice Statement of Public Key Infrastructure of Aristotle University of Thessaloniki

Version 3.4 (April 23rd 2012)

Document Manager: Dimitris Zacharopoulos

Working Group: Dimitris Zacharopoulos
Dimitris Daskopoulos
Kyriaki Lambridou

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).

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 AUTH PKI also complies with the following more general rules and procedures, depending on the type of the certificate.

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.

The globally unique Identification Number (OID) of this document is: 1.3.6.1.4.1.**7709.2.0.3.4** 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
3.4	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 is 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 validity period of the certificates of the Subordinate Certification Authorities is **four (4) years**. Initially, operate:

- One (1) subordinate Certification Authority for the entities that manage the AUTH PKI; which is, the AUTH Network Operations Center (AUTH-NOC-CA). AUTH-NOC-CA issues certificates for users and servers/devices of AUTH NOC, but not for entities of other units.
- Two (2) subordinate Certification Authorities for entities of the academic and administration units of the University (AUTH-SUBSCRIBERS-CA and AUTH-SERVERS-CA) that issue certificates for users and servers/devices respectively .

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 NOC is the central Registration Authority of PKI and applies strict procedures for users’ authentication.

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 relationship with AUTH and devices operated by AUTH).

The subscription of roles (e.g. 'Rector') or persons that are not real, apart from network devices or services, is neither explicitly foreseen in the current document nor forbidden. The issuance of 'role certificates' is possible by a subordinate CA, provided that the relevant procedure is described in the CP/CPS of the corresponding subordinate CA and that this procedure does not conflict with any condition of the current document.

1.3.4 Relying Parties

The entities that trust the provided certification services or otherwise called the Relying Parties or simply 'users' of the certification services can be any entity, inside or outside the Hellenic academic community, which uses in any way the certification tokens (digital certificates, digital signatures, time stamps etc) and relies on the information that they contain.

In particular, entities that trust the Certification Services Provider (CSP) are the persons or legal entities who, after being informed and having agreed with the terms and conditions concerning the use of the certificates as described in the present document and the relative certificate policy, and after having checked and verified the validity of a certificate that has been issued by the CSP of AUTH PKI, they decide whether they can rely on the content of this certificate in order to proceed to specific actions or justified belief.

In order to verify the validity of the certificate, the user must check that:

- √ The validity period of the certificate has begun and has not expired.
- √ The certificate is correctly signed by a Trusted Certification Authority.
- √ The certificate has not been revoked for any reason.
- √ Subject identification matches the details that the signer presents.
- √ The usage for which the certificate is presented and is according to the reason it was issued by the CA
- √ Abides by the terms and the conditions that are described in the present Certification Practice Statement

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 as described in paragraph 1.3.

1.4.1 Appropriate certificate uses

The certificates can be used only for academic and research purposes, in all network services and applications in which the required level of security is equal or lower than that of the certificate issuance process.

Typical applications in which digital certificates issued by the Certification Services Provider Service, can be used, are the following (the list is not restrictive):

a) Signing of an “electronic document” by a person using her/his digital certificate and the relevant private key, preferably with the use of a “secure mechanism for signature creation” (e.g. smart card or e-token), so that at least the following characteristics are ensured: 1) the authenticity of origin, 2) the integrity of the signed document i.e. that its content has not been modified since the time of its’ signature and 3) the binding of the signer to the content of document and the non-repudiation of signature.

b) Signing of e-mail messages, as a proof of authenticity of the sender’s address and for all the attributes described in (a). Moreover, they can be used for the purpose of secure proof of receipt of messages (non-repudiation of receipt).

c) Persistent proof of identity (Strong Authentication) of a person or a device throughout communication with other entities, guaranteeing high level security characteristics, stronger than the ones that are provided by the password-based access control method.

d) “Encryption of documents and messages” with the use of the recipient’s public key, ensuring that only she/he, the holder of corresponding private key, can decipher and read the document or the message.

e) Certification of other Certificate Services Provider such as a Subordinate CA or other additional services of certification, e.g. time-stamping, digital notarization and long-term secure preservation of data.

f) In the implementation of secure network protocols, such as SSL, DNSsec, IPSec etc.

1.4.2 Forbidden Certificate Use

Certificates cannot be used for commercial or financial transactions or for transactions that include any legal bindings.

1.5 Policy administration

1.5.1 Policy Making Organization

ca-admin@ccf.auth.gr
Network Operations Centre of AUTH
Faculty of Sciences
1st floor of the Biology Department Building
University campus of AUTH
54124 Thessaloniki,
Greece

1.5.2 Contact Persons

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

Dimitris Daskopoulos [dimitris@ccf.auth.gr]
Tel: 2310 998490
Fax: 2310 998492

Network Operations Centre 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@ccf.auth.gr]

Tel: 2310 998483

Fax: 2310 998492

Dimitris Daskopoulos [dimitris@ccf.auth.gr]

Tel: 2310 998490

Fax: 2310 998492

Network Operations Centre 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 Communication Networks and Informatics Steering Committee of Aristotle University of Thessaloniki.

1.6 Definitions and Acronyms

English term	Abbreviation
Object Identifier	OID
Registration Authority	RA
Policy Certification Authority	PCA
Certification Authority	CA
Certification Practice Statement	CPS
Public Key	
Certification Path	
Distinguished Name	DN
Trusted Third Party	TTP
Private Key	
Hierarchic Certification Structure	HCS
CommonName	CN
Certificate Revocation List	CRL
Certification Trust List	CTL
Organization Name	O
Organizational Unit	OU
Country Name	C
Certificate	
Certification Policy	CP
Public Key Infrastructure	PKI
Certificate Subject	
Certification Authority Digital Certificates	
Server Digital Certificates	
Personal Identity Digital Certificates	

Object-Signing Digital Certificates	
Public-Key Cryptography Standards	PKCS
Subscriber	
Relying Party	
Data Repository	
Self signed certificates	
Identification	
Authentication	
Private Key Escrow	
Policy Qualifier	
Secure Socket Layer	SSL
Uniform Resource Identifier	URI

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 CRL is updated according to the paragraph 4.9.7.

The certificates that are issued by the CA, are being published immediately after their retrieval from the subscriber.

2.4 Access control

The repository section containing the certificates is publically available through a search web page. The search is performed either by entering the certificate serial number (therefore a single certificate is returned), or by entering part of the distinguished name of the certificate subject (therefore a list of certificates is likely to be returned).

Restrictions may be applied to the repository access to protect it against enumeration attacks.

3 Identification and Authentication

3.1 Terminology

The names that are used for the certificate issuance depend on the class of the certificate and they are according to the X.500 standard.

3.1.1 Name Types

3.1.1.1 User Certificates

The user certificates must include the full name of the user, his e-mail address (according to rfc822), the name of the entity she/he belongs to, and the abbreviation o=Aristotle University of Thessaloniki.

Optionally, additional fields may be included, such as the organizational subunit the user belongs to and her/his location.

3.1.1.2 Device/Services Certificates

Certificates that are issued for appliances (server, router or any other network device) must include the complete distinguished name of the

appliance according to the Domain Name System (FQDN DNS), the name of the unit it belongs to, and the mark “o=Aristotle University of Thessaloniki, c=gr”. The certification of IP addresses or hostnames instead of the FQDNs is not allowed.

Optionally, additional fields may be included, such as the organizational sub-unit and the device’s location.

3.1.2 Obligation for meaningful names

The names that are included in the user certificates must be related to the subscriber/recipient of the certificate.

3.1.3 Anonymity or pseudonymity of subscribers

The AUTH-PKI does not allow certificate issuance for anonymous users. The certificate issuance for pseudonyms in the distinguished name e.g. “Rector”, is not foreseen in the present Certification Practice Statement but it is also not prohibited. A special purpose intermediate Certification Authority can be created for these types of distinguished names.

3.1.4 Rules for interpreting various name forms

The names are composed according to the certificate type. The subscriber’s name that is composed according to the rules of the current section is called Distinguished Name (DN).

3.1.4.1 User Certificates

Regarding the user certificates, the field that includes the name of a user corresponds to the characteristic “CN”, the e-mail to “E”, the institution she/he belongs to “O” or/and “OU”, the country to “C” and optionally the location it is found to “L”. It is preferable to adapt to the naming conventions used by the national directory service (today it is hosted at ds.grnet.gr). The AUTH User Certificates must include the characteristics “O=Aristotle University of Thessaloniki, C=GR” in the Distinguished Name.

3.1.4.2 Device/Services Certificates

The name of the device certificate (FQDN DNS) corresponds to the characteristic “CN”, the name of the unit that the device belongs to corresponds to the characteristic “OU”, the name of the Organization corresponds to the characteristic “O”, the country corresponds to the characteristic “C” and optionally, the location corresponds to the characteristic «L». The AUTH Device Certificates must include the characteristics “O=Aristotle University of Thessaloniki, C=GR” in the Distinguished Name.

3.1.4.3 Code Signing certificates

Code Signing certificates are provided through user certificates described in section 3.1.4.1. The user, in addition to the general terms-and-conditions of simple user certificates, is committed (via an appropriate extra RA agreement) to provide complete, accurate and truthful information (eg, application name, information URL, application description, etc.) in the digitally signed code.

The digital signing of malicious code (malware) is expressly prohibited.

Failure by a Subscriber to comply may result in revocation of the code signing certificate.

3.1.5 Uniqueness of Names

The distinguished name of a subscriber bearing attributes of AUTH must be unique for the particular Certification Authority that issues the certificate, while it is desirable to be unique in the entire hierarchy of certification of AUTH. The issuance of more certificates with the same DN is allowed only in case of different class or certificate usage.

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 Council, after the recommendation of the Communication Networks and Informatics Steering Committee of Aristotle University of Thessaloniki.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

The Registration Authority must verify that the alleged subscriber really possesses the private key that corresponds to the public key of the about-to-be-issued certificate. This is achieved with the following process:

- The identity of the subscriber is authenticated.
- An application for certificate issuance is submitted. The application contains the public key of the subscriber and has been signed with the private key of subscriber
- The key matching is verified.

3.2.2 Authentication of organization identity

The Registration Authority must confirm that the subscriber belongs to the Aristotle University of Thessaloniki. The name of AUTH is included in the certificate. The subscriber must:

a) be registered in the official directory service of the University or
b) Possess an e-mail address in the official mail service of AUTH and the administration services of AUTH must confirm the relationship with the subscriber.

3.2.3 Authentication of individual person identity

3.2.3.1 Entity applying for the issue of a certificate

The certificates of individuals that are issued by AUTH 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). Note that there is a secure identification of the recipient with

her/his physical presence and an acceptable official document proving his identity in both classes of certificates.

The Registration Authority relies on the control of identity performed by the academic/administration units the subscriber belongs to and uses authentication ways of user identities that are available in these units in order to check the identity. The collaborating academic/administration units are compelled to have certified user's identity by means of an official document that bears the photograph of the beneficiary (e.g. police identity, passport, driving license, student identity, no student public transportation card "PASO"), which is considered reliable by the corresponding unit. Alternatively, the RA of AUTH can execute the above process of applicant identification.

In case the user's academic/administration unit has already performed a procedure of physical identity verification in the past, according to its policy (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 user's e-mail address is sufficient.

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'.

3.2.3.2 Individual who applies for a device certificate

The individual who is in charge of the operation of the device and its conformity to the Certification Policy should possess a certificate issued by a CA that conforms to the "AUTH Certification Practice Statement/ Certification Policy".

The subscriber submits the application for a device certificate on a web interface where she/he must be authenticated presenting her/his personal certificate.

After this, a verification e-mail is sent to the RA's designated administrator who verifies the validity of the FQDN of the certificate request.

He also checks that the person who applied for the certificate is the rightful owner of the FQDN according to AUTH database of users / servers.

3.2.4 Non verified subscriber information

The certificates that are issued do not include non-verified subscriber information.

3.2.5 Validation of subscriber status

The Registration Authorities determine procedures according to which the subscriber's status and his relationship with AUTH are being verified. This is possible either with electronic lists assembled by each RA from the qualified - for each category- sources (e.g. secretariats of departments /faculties, AUTH central registry etc.), or by presenting official certificates where the relationship of the subscriber with AUTH is certified.

3.2.6 Criteria for interoperability

Not defined.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication for routine re-key

The user can request the issuance of a Re-key/Certificate fifteen **(15) days** before the expiry of the existing certificate, following the described procedures in section 3.2.

3.3.2 Identification and Authorization for Re-key after revocation

The user can request the issuance of a Re-key after the revocation of the initial certificate, following the described procedures in section 3.2.

3.3.3 Identification and authentication for revocation requests

As stated in paragraph 3.2.3. Moreover, the CA and the subscriber agree to a secret revocation code during the retrieval of the certificate. The subscriber can require the revocation of the certificate through the appropriate web interface, using the secret revocation code. Alternatively, a certificate revocation can be asked by the subscriber making a call to the appropriate Certification Authority therefore his identity must be verified.

4 Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who is eligible to submit a certificate application

Applications for certificate issuance may be submitted only by the subscribers as described in paragraph 1.3.3.

4.1.2 Enrollment process and responsibilities

The applicant's certificate DN must be according to section 3.1. The validation of a user identity must be according to section 3.

The subscriber submits the application for certificate issuance through the web page of the Registration Authority, http://www.pki.auth.gr/ or through the RA of her/his AUTH School or Faculty in accordance with the section 9.16.2.

4.2 Certificate Application Processing

4.2.1 Subscriber identification and authentication procedures

The processing of the applications is based on what is outlined in section 3.2. All certificate applications are checked for validity. The subscriber's identity and official relationship with AUTH are also checked.

4.2.2 Approval or rejection of certificate applications

After the identity/attribute checks of the applicant, the content of the application for the digital certificate is also checked. In case the applicant is not eligible for a digital certificate or the digital application contains faults, the application is rejected. Otherwise the application is approved.

4.2.3 Time to process certificate applications

The certificate applications are processed within a period of ten (10) working days maximum, apart from the cases of force majeure.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate issuance

The certificates are issued after the secure transmission of applications from the Registration Authority to the Certification Authority and after the

verification of the DN of the certificate. The DN of the certificate of the applicant must agree with the specifications outlined in section 3.1.

4.3.2 Notification to subscribers by the CA regarding certificate issuance

The Certification Authority notifies the subscriber about the success or rejection of the certificate issuance via e-mail. In the same e-mail message, provided that the application is accepted, a unique URI is sent to the subscriber who must accept the terms and services of AUTH PKI before accepting and receiving the issued certificate.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The AUTH-PKI subscribers must accept (retrieve and install through a secure webpage) the new certificate within thirty (30) days, otherwise the Certificate is automatically revoked and the subscriber must repeat the application process. The subscribers must declare on the secure webpage that they have checked all certificate elements and that they are correct, in order to retrieve their certificate. Finally, they accept and receive the certificate.

4.4.2 Publication of the certificate by the CA

All CAs publish the certificates only after they have been retrieved by the owners according to section 4.4.1.

4.4.3 Notification of other entities about certificate issuance by the CA

No action is taken for the notification of other entities other than what is stated in section 9.16.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private keys and certificate usage

The AUTH-PKI subscribers are allowed to use their private keys and certificates for the usages stated in section 6.1.7.

4.5.2 Relying party public keys and certificate usage

Relying parties can use the AUTH-PKI subscribers' public keys and certificates following what was stated in section 1.3.4. The operations they can execute are:

- Verification of digitally signed e-mail messages using the S/MIME protocol
- Encryption of e-mail messages using the S/MIME protocol
- Verification of digitally signed documents/application code
- Verification of digital timestamps in documents
- Encryption of files, data and communication channels
- Authentication
- Authorization

4.6 Certificate Renewal

4.6.1 Prerequisite Circumstances for certificate renewal

Certificate renewals are allowed provided that the key lifetime of the certificates is not exceeded. Furthermore, everything listed in section 1.3.3 applies. The lifetimes are stated in section 6.3.2.

4.6.2 Who may request certificate renewal

The renewal request is submitted by the subscriber choosing renewal through a secure web page after authentication.

4.6.3 Processing certificate renewal requests

- Initially, a check whether renewals of the same certificate were made in the past takes place.
- Afterwards, a check whether the certificate or the certificates that contain the same key, exist for a smaller duration than the maximum validity period takes place.
- For the rest of the permitted time period a new certificate is issued using the initial certificate request which is stored in the Registration Authority.

For instance, a user who has an existing certificate with one year validity period can renew it (without changing the private key) for another year,

because the maximum validity period of the private key is **two (2) years** for user certificates.

4.6.4 Notification of new certificate issuance to subscriber

The same new certificate issuance procedure is followed, as stated in section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

The user/subscriber should receive the new certificate following the same procedure of acceptance and receipt of the new certificate, as stated in section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

The new certificate is published according to the procedures stated in section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

No action is taken for the notification of other entities other than what is stated in section 9.16.

4.7 Certificate Re-keying

4.7.1 Circumstances for certificate re-keying

Certificate Re-Keys are permitted when the certificate is almost expired or the certificate is revoked and a new one should be issued.

4.7.2 Who may request certification of a new public key

The beneficiary subscribers receive an e-mail message from the Registration Authority **fifteen (15)** days before the expiry date of their certificate and are informed for its imminent expiry. The subscribers afterwards make a Certificate Re-key request via a secure web page, after authenticating, in which they choose Re-key issuance.

4.7.3 Processing certificate re-keying requests

The same Re-key issuance procedure is followed, as stated in section 4.3.

4.7.4 Notification of the new certificate to subscriber

The same Re-key issuance procedure is followed, as stated in section 4.3.2

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The user/subscriber must receive the certificate with the new key, following the same acceptance procedure, as described in section 4.4.1.

4.7.6 Publication of the Re-keyed certificate by the CA

The certificate with the new key is published, according to the repository procedures, as stated in section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

No action is taken for notification to other entities other than what is stated in section 9.16.

4.8 Certificate Modification

4.8.1 Circumstances for certificate modification

Modification of certificate details is not permitted. In case there is a mistake during certificate issuance (spelling or something else), the certificate is revoked and the Re-key issuance process is followed, as stated in section 4.3.

4.8.2 How can be requested a certificate modification

Modification of certificate information is not permitted.

4.8.3 Processing certificate modification requests

Modification of certificate information is not permitted.

4.8.4 Notification of new certificate issuance to subscriber

Modification of certificate information is not permitted.

4.8.5 Conduct constituting acceptance of the certificate

Modification of certificate information is not permitted.

4.8.6 Publication of the modified certificate by the CA

Modification of certificate information is not permitted.

4.8.7 Notification of modified certificate issuance by the CA to other entities

Modification of certificate information is not permitted.

4.9 Certificate Suspension and Revocation

4.9.1 Circumstances for revocation

A certificate is revoked when it is not used any more, when the fields it contains have changed or when the corresponding private key has been exposed or lost or when there is suspicion that it has been exposed or lost. Moreover, the certificate is revoked when the subscriber has not accepted it in the time interval that is defined in section 4.4.1or if it has been proven that the usage of the certificate does not conform to the certification policy. Finally, it is revoked if it contains erroneous information.

The loss of applicant's attribute or relationship, labor or other, with Aristotle University of Thessaloniki or the specific unit she/he belonged to when she/he was verified (e.g. graduation, termination of employment), is a revocation reason as well.

4.9.2 Who can request a revocation

The certificate can be revoked by the subscriber or by another entity that can prove the exposure or the misuse of the certificate according to the Certification Policy.

The secretariats or personnel services of the units of AUTH are obliged to make revocation request for persons who lost their attribute under which they were verified.

4.9.3 Procedure for revocation request

4.9.3.1 Certificate revocation by the subscriber

The validation of the subscriber's identity is required according to section 3.3.3.

4.9.3.2 Certificate revocation by any other entity

Submission of proof that

a) the private key of the certificate has been exposed, or

b) the use of the certificate does not conform to the Certification Policy, or

c) the certificate owner's relationship with AUTH does not exist any more,

is required.

4.9.4 Revocation request grace period

The subscriber can make a revocation request anytime during the validity period of the certificate. Certificate revocations can take place if the CA which issued these certificates is still in operation.

4.9.5 Time within which CA must process the revocation request

The Certification Authorities must process the revocation requests within one (1) working day except from force majeure cases.

4.9.6 Revocation checking requirements for relying parties

Relying parties must follow the described procedures in section 1.3.4 before they rely on any certificate. They should load the Certificate Revocation Lists of all intermediate Certification Authorities that intervene. The revocation lists are always published in the Repository.

4.9.7 CRL issuance frequency

The CRL will be issued at least every five (5) days. The CRL will be in effect for five (5) days.

In case of subscriber's private key exposure or any other important security compromise an updated CRL will be issued immediately.

4.9.8 Maximum latency for CRLs

After a certificate revocation, the CRL is issued and the repository is updated. The CRL is published at the Repository within minutes of its issuance. The certificate is marked as revoked in the Repository.

The subscriber and the person in charge of the CA security are notified in case of exposure of the private key during the certificate revocation.

4.9.9 On-line revocation/status checking availability (OCSP)

An On-line Certificate Status Protocol – OCSP service operates under PKI-AUTH. The URL of this service is included in the issued certificates.

4.9.10 Online revocation checking requirements

Relying Parties must follow the procedures in section 1.3.4 before relying on any certificate. They must also check every time, the OCSP service of AUTH-PKI and inquire the status of all intermediate CAs that intervene. The URL of the OCSP service is included in all issued certificates.

4.9.11 Other forms of revocation advertisements available

The revoked certificates appear as “Revoked” in the search engine of Certificate Repository.

4.9.12 Special requirements re-key compromise

As defined in section 4.9.3.2.

4.9.13 Circumstances for suspension

Certificate suspension is not provided.

4.9.14 Who can request suspension

Certificate suspension is not provided.

4.9.15 Procedure for suspension request

Certificate suspension is not provided.

4.9.16 Limits on suspension period

Certificate suspension is not provided.

4.10 Certificate status services

4.10.1 Operational characteristics

Relying parties can use one of the following offered services or a combination of them, in order to decide for the validity of some certificates.

4.10.1.1 Online Certificate status service OCSP

As defined in section 4.9.10.

4.10.1.2 On-line Certificate Repository

The online Certificate Repository offers a web-based certificate search engine, supporting queries that contain the serial number or a part of the Distinguished Name of the certificate. The search results include the information of the certificate and an indication on whether the certificate is valid or if it has been revoked. The Certificate Repository must display all certificates issued / revoked for as long as AUTH PKI is operational.

4.10.1.3 Usage of Certificate Revocation Lists (CRL)

As defined in section 4.9.6.

4.10.2 Service availability

The CA performs all the necessary actions for the uninterruptible - as possible - availability of its OCSP service (~99%).

4.10.3 Optional features

Not defined.

4.11 End of subscription

After the end of validity of AUTH-PKI certificates, the revocation is not necessary unless there is a reason such as the ones referred in section 4.9.1.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

Not defined.

4.12.2 Session key encapsulation and recovery policy and practices

Not defined.

5 Administrative, Technical and Operational Controls

5.1 Physical security and access controls

5.1.1 Site location

The Central Certification Authority of AUTH is currently located at the Network Operation Center of the Aristotle University of Thessaloniki premises, on the 1st floor of the building of Biology, Faculty of Sciences, Aristotle University of Thessaloniki. Other subordinate Certification Authorities may be located inside and outside AUTH NOC.

5.1.2 Physical access

Physical access to the equipment of the CAs and the RAs is only allowed to authorized personnel. The connection of the Central CA to any telecommunication network is prohibited.

5.1.3 Power and cooling

All equipment of the AUTH PKI currently hosted at AUTH NOC, is in air-conditioned rooms with power supply protected by Uninterruptible Power Supply units (UPS) and backup power generators.

5.1.4 Water exposures

The equipment of AUTH PKI currently hosted at AUTH NOC premises is not at serious risk of flood.

5.1.5 Fire prevention and protection

AUTH NOC premises meet the Greek law on prevention and fire protection in public buildings.

5.1.6 Media storage

The private keys of Certification Authorities must be stored in external storage media (e.g. CD-Roms) or other removable media in encrypted form, with a passphrase that is distributed in parts only to authorized personnel. No single member of the authorized personnel has the full passphrase to decrypt a private key.

Backup of the entire Public Key Infrastructure of AUTH, is kept on tape or memory flash disks kept by qualified executives.

Both of the previously mentioned storage media are in different physical locations, outside of the central servers of NOC AUTH, protected from exposure to water and fire.

5.1.7 Waste Disposal

Waste containing any confidential information, such as floppy disks, hard disks etc. are destroyed before being discarded.

5.1.8 Off-site backup

There are off-site backups of all servers of NOC AUTH. The private key of each CA is always stored encrypted. The decryption passphrase is only known to the authorized personnel of each CA. The private keys of the Certification Authorities managed by NOC AUTH are stored in detachable storage media. A backup of the entire Public Key Infrastructure of AUTH is stored in a magnetic tape held by authorized personnel. No single member of the authorized personnel possesses the private key and the complete passphrase to decrypt the private key at the same time.

Both of the previously mentioned storage media are in different physical locations, outside of the central servers of NOC AUTH, protected from exposure to water and fire.

5.2 Procedural controls

5.2.1 Trusted roles

The personnel assigned to operate the CAs is considered to be trusted and authorized to perform all the works of the Certification and Registration Authorities. Personnel assigned to administer the servers of the Registration Authorities are authorized to back up the transaction log files.

5.2.2 Number of persons required per task

Not defined.

5.2.3 Identification and authentication for each role

Not defined.

5.2.4 Roles requiring separation of duties

Not defined.

5.3 Personnel controls

5.3.1 Qualifications, experience and clearance requirements

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.

5.3.2 Background check procedures

Personnel handling Certification Authorities and Registration Authorities comply with the applicable laws and framework.

5.3.3 Training requirements

Personnel operating the CA and the RA and has access to cryptographic procedures, is trained and educated on issues of the Public Key Infrastructure of AUTH by technicians of NOC AUTH. For this purpose there is adequate documentation that describes all the operational procedures of the infrastructure. Personnel working within the AUTH PKI needs to know all policy / procedures documents, and the Certificate Practice Statement and the Certification Policy of the AUTH PKI in particular.

5.3.4 Re-training frequency and requirements

Not defined.

5.3.5 Job rotation frequency and sequence

Not defined.

5.3.6 Sanctions for unauthorized actions

All legal procedures prescribed for certain offenses and the AUTH Network Policy are followed.

5.3.7 Independent contractors requirements working outside AUTH and involved with the AUTH PKI

In case AUTH PKI hires an independent contractor for audit or other operations, the contractor is obliged to sign a Non Disclosure Agreement contract. The same principle applies for external auditors.

5.3.8 Documentation supplied to the personnel

Relevant documentation is available from NOC AUTH and offered to trainees who undertake specific roles within the AUTH PKI.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The AUTH PKI systems record applications for certificates, the certificates and the CRLs that are being issued and the messages exchanged with the Registration Authority. Furthermore, in all AUTH PKI servers, other processes of the operating system and applications are recorded such as connections and disconnections of the administrators, HTTP connections to web servers, etc. All servers that record logs are synchronized via NTP (Network Time Protocol) as described in section 6.8.

5.4.2 Frequency of processing log

All transactions are archived in a daily basis.

5.4.3 Retention period for audit log

The transactions-events files are kept for **two (2)** years in order to be available for any lawful control. This period may be modified depending on developments of relevant laws.

5.4.4 Protection of audit log

Access to the transactions file in general is prohibited. Only reading and addition by authorized systems and authorized personnel is allowed. Deletion of file entries is not allowed.

5.4.4.1 Access

Access to the transactions file is allowed only for reading to certain applications of the CAs and RAs and to authorized personnel.

5.4.4.2 Protection against changes in transactions file

An access policy is applied that allows changes only to the administrators of the operating system of the CA and the RA.

5.4.4.3 Protection against deletions in transactions file

An access policy that allows changes only to the administrators of the operating system of the CA and the RA, is applied.

5.4.5 Audit log backup procedures

A backup of the transactions-events file is kept.

5.4.6 Audit collection system (internal vs. external)

Not defined.

5.4.7 Notification to event-causing subject

Not defined.

5.4.8 Vulnerability assessments

Not defined.

5.5 Records Archival

5.5.1 Types of records archived

All records of transactions referred in section 5.4, and all documentation related to requests for issuance / revocation of digital certificates are archived.

5.5.2 Retention period for archive

The records file is kept for **two (2) years** in order to be available for any lawful control. This period may be modified depending on developments of the relevant legislation.

5.5.3 Protection of archive

Access to the records file in general is prohibited. Only reading by authorized systems and authorized personnel is allowed. No changes or cancellations of the records of the file are allowed.

5.5.3.1 Access

Only authorized personnel may access the records file.

5.5.3.2 Protection against the alteration of the records file

An access policy which does not allow changes is applied.

5.5.3.3 Protection against the deletion of the records file

An access policy which does not allow deletions is applied.

5.5.3.4 Protection against the deterioration of storage media

Not defined.

5.5.3.5 Protection against future lack of availability of readers of the old media

Not defined.

5.5.4 Archive backup procedures

A backup of the records files is kept.

5.5.5 Requirements for time-stamping of records

Currently, the time stamping of the records files is not required.

5.5.6 Archive collection system (internal or external)

Not defined.

5.5.7 Procedures to obtain and verify archive information

Not defined.

5.6 Key changeover

In case a certification authority key is changed, the keys of the final certificates must be revoked and recreated according to the procedures in section 4.1.

5.7 Compromise and disaster Recovery

5.7.1 Incident and compromise handling procedures

The logs are periodically monitored to detect security breaches of systems and subsystems. If an abnormality or a suspected violation is detected, the service is suspended and a thorough check of all systems takes place.

5.7.2 Computing resources, software and/or data are corrupted

In case of suspected violation, the service is suspended and a thorough check of all systems takes place. If a violation is confirmed, a check is done whether there is infringement on private keys. In case of violation without loss of private keys, the system is restored from backups where there is no suspicion of violation, new security checks take place to find potential security holes and then the service returns. In case of lost keys, the procedures of the next paragraph are followed.

5.7.3 Entity private key compromise procedures

In case of loss of private keys, final certificates are revoked by the certification authority and issuance of new is done without interruption of the service. In case of private key loss of a subordinate Certification Authority, all subscribers of this subordinate Certification Authority are notified, all final certificates issued by this Certification Authority are revoked, along with the certificate of the Certification Authority. If the private key of the Central Certification Authority is lost, each CA must stop the service, notify all subscribers of all subordinate Certification Authorities, proceed with the revocation of all certificates, issue a final CRL and then notify the relevant security contacts. Then the Public Key Infrastructure will be set up again with new Certification Authorities starting with a new Central Certification Authority.

5.7.4 Business continuity capabilities after a disaster

The AUTH PKI has the ability to operate continuously using backups of all systems/subsystems in a location outside the premises of the AUTH servers.

5.8 Certification Authority or Registration Authority termination

Upon its termination, each CA informs its subscribers, revokes all issued certificates, updates the relevant CRL and revokes its own certificate. Finally, the persons in charge of the CA security are informed and the end of its operation is announced. The log files of the CA and RA are kept for two (2) years in order to be available for any lawful control. This period may be modified depending on the relevant legislation.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The keys of the subscribers are generated by hardware and software at the candidate subscribers' side and remain under their absolute control throughout their period of validity. If the procedures of a Certification Authority allow the mass creation of keys for third parties, there must be a procedure for the destruction of all copies of the private keys after their delivery to the users in order for the private keys to be under the possession of the recipient subscribers only. In case a subscriber wishes to obtain a Class A certificate, as described in section 3.2.3.1, she/he must submit the application under the presence of an authorized person of the Registration Authority to certify the usage of a crypto-token hardware device.

The keys of the CAs are generated by special software or hardware cryptographic devices (eToken, smartcard) that are installed in the CAs. These cryptographic devices must comply with the FIPS 140-2 standard. Checks must be performed during the creation of the keys in order to identify the existence of bugs in software or hardware used, involving the creation of keys.

6.1.2 Private Key delivery to subscriber

The creation of private keys by any entity on behalf of the candidate subscriber or another entity or from the CA on behalf of the subscribers is not allowed. The delivery of the private key of the candidate subscriber to any

third entity is not allowed. If a Certification Authority allows the creation of private keys on behalf of another entity, the following procedure must take place:

- If the CA has enough information to confirm the validity of the identity of the user in advance, it has the ability to generate a key pair and a certificate for this user.
- The verification of the authenticity of this certificate is implemented when owners receive the credentials (certificate and keys) from the RA. This model is called collective.
- The CA must have a procedure to delete the secret key associated with each certificate the moment it is delivered to the subscriber, so that eventually, the private key is in possession of the subscriber only.

6.1.3 Public key delivery to certificate issuer

The subscriber must submit his public key to the Registration Authority through a structured application (e.g. format PKCS#10) for certificate issuance. The request is signed with the relevant private key. The RA verifies a) the correctness of the signature and b) that the applicant is in possession of the corresponding private key.

6.1.4 CA public key delivery to relying parties

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.

Each CA publishes its certificate at the certificate store describe in section 2.1.

6.1.5 Key sizes

The minimum allowed key size is 2048 bits regardless of the use.

6.1.6 Public key generation parameters and quality checking

Not defined.

6.1.7 Key usage purposes as per X.509 key usage field

The intended use of a key is referred by the designated basic field and the designated extension of the X509v3 type of certificate. The certificate usage purposes are not restrictive (i.e. non-critical certificate extension) but "suggested". Monitoring compliance with the authorized purposes usage is at the discretion of relevant parties.

Depending on the certificate class, certificate fields include at least the following uses:

Personal user certificate class:

Basic usages: 'Digital Signature', 'Non-Repudiation', 'Data Encipherment', 'Key Encipherment'.

Extensions: 'Client Authentication', 'Secure Email', 'Encrypting File System'

Device certificate class:

Basic usages: 'Digital Signature', 'Key Encipherment'.

Extensions: 'Client Authentication', 'Server Authentication'

Certificates with additional special services class:

Extensions: 'IP Security User', 'Timestamping', 'Code Signing', 'OCSPSigning'

6.2 Private key protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Not defined.

6.2.2 Private Key control from multiple persons (N out of M)

The activation code of the private key of every CA is segmented using a method described in an internal AUTH PKI document.

6.2.3 Private Key escrow

Not defined.

6.2.4 Private Key backup

The private key of every CA must be kept at a backup copy. The backup copy of the private key must be encrypted and the procedures

referenced at section 5.1.6 must be followed. Access to the backup copy is allowed only by authorized personnel.

6.2.5 Private Key archival

The backup copy of the private key of each Certification Authority must be archived and kept using secure methods at a secure place. Private keys at the backup copy are always encrypted but there is an additional encryption protection of all archived backup copies. Furthermore, all procedures described at section 5.1.6 are followed. Access to the archived backup copy is allowed only by authorized personnel.

6.2.6 Private Key transfer into or from a cryptographic module

Owners of private keys may transfer their private key from a software certificate store to any hardware cryptographic device, e.g. crypto-tokens, smartcards. This procedure does not change the class of the certificate from B to A since the private key was not generated originally at the hardware cryptographic device. The reverse procedure (transfer of the private key from a hardware device to a software certificate store) is not allowed.

6.2.7 Private Key storage on cryptographic module

Not defined.

6.2.8 Methods of activating private key

6.2.8.1 Who can activate (use) a private key

The private key of every CA is protected (encrypted) with a passphrase. Each authorized person knows a different part of the passphrase. Only a combination of authorized personnel can decrypt the private key of each CA in order to perform cryptographic procedures. The procedure is described in an internal AUTH PKI document, which describes the ‘ceremony to activate Certification Authorities’.

The private key of user and device certificates must also be protected-encrypted. Only the owner or administrator of the device or service may activate and use a private key that corresponds to the certificate.

6.2.8.2 Actions to be performed to activate a private key

In order to activate a private key, a passphrase must be entered to decrypt and use the private key in combination with the certificate. In case of hardware cryptographic device (e.g. crypto-tokens) a specific PIN is required.

For CA private key activation that is stored in crypto-tokens, a combination of codes is required. Each authorized administrator knows a different part of the activation PIN. Only a combination of the authorized personnel can activate a private key.

In case of end user certificates that are stored in software certificate stores (e.g. CryptoAPI at MS Windows), a passphrase may not be required but a simple question of whether or not to use the private key. Finally, private keys used in devices-services may be permanently activated and not protected at all by using a passphrase, as long as there are other sufficient security measures at the file system level (file system permissions) or other security precautions.

6.2.8.3 Once activated, for how long is the key «active»;

Not defined. Usually the key stays «active» for as long as the particular application that uses the certificate, is active.

6.2.9 Methods for deactivating private key

Not defined.

6.2.10 Methods for destroying private key

Not defined.

6.2.11 Cryptographic module rating

Not defined.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are embedded within the digital certificates during their issuance and are archived according to the procedures defined in sections 5.4 and 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The key pair operational period is defined by the operational period of the corresponding digital certificate. The maximum operational period of the keys is defined as **eight (8)** years for the Central CA, **four (4)** years for a Subordinate CA and **two (2)** for end user and device certificates. The operational period must be defined according to the size of the keys and the current technological developments at the field of cryptography, so that the best level of security and efficiency of use is guaranteed.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data (passphrases and PINs) must be chosen in such a way so that it is difficult to be discovered. The minimum size of the passphrase and the PIN is **eight (8)** digits.

In case there is an embedded private key destruction mechanism after a certain number of incorrect entries, then the PIN size may be smaller. In any case, the procedures defined in section 6.2.8 are used.

6.4.2 Activation data protection

Not defined.

6.4.3 Other aspects of activation data

Not defined.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

- The Operating Systems of the computers of the AUTH PKI are kept in high security level with the implementation of international standards and security guidelines.
- There are logging systems at the computers of the AUTH PKI which are checked on a regular basis and the log files are scrutinized periodically in order to identify potential anomalies.
- Only the absolutely necessary programs/applications for the correct operation of the RA/CA are installed within the Operating System.

6.5.2 Computer security rating

Not defined.

6.6 Life cycle technical controls

6.6.1 System development controls

Not defined.

6.6.2 Security management controls

Not defined.

6.6.3 Life cycle security controls

Not defined.

6.7 Network security controls

The connection of CAs to wider data networks or other telecommunication media (e.g. the telephone network using a modem) is not allowed. The Registration Authority is protected from the internet using strong security mechanisms including firewalls.

6.8 Time-stamping

All time-stamping services -including logging operations- at AUTH PKI (either at the RA or the CA operations) must be synchronized via NTP (Network Time Protocol).

7 Certificate, CRL and OCSP Profiles

7.1 Certificate profile

A certificate profile according to RFC 3280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile” is used.

7.1.1 Version number

The version number of the certificates is 2, which corresponds to X.509v3 certificates.

7.1.2 Certificate extensions

Every issued certificate must include the BasicConstraints extension marked as critical and the KeyUsage, SubjectKeyIdentifier and CertificatePolicies extensions marked as non-critical. Furthermore, the CRLDistributionPoint extension must be included marked as non-critical.

7.1.3 Algorithm object identifiers

The signature algorithm must be SHA1 or stronger. Use of MD5 is prohibited along with other hashing algorithms that have been compromised.

7.1.4 Name forms

The name form is done according the rules of section 3.1

7.1.5 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”, “edu”, “eu” domains.

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

7.1.6 Certificate policy object identifier

The OID (Object Identifier) of the certificate policy 1.3.6.1.4.1.7709.2.0.3.4, which complies with the CP/CPS of AUTH PKI, version 3.4, is included in the certificates.

7.1.7 Usage of Policy Constraints extension

Not defined.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifier is the URI which points to the published CP/CPS of AUTH PKI.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not defined.

7.2 CRL Profile

7.2.1 Version number

The version number is 1 or/and 2, which corresponds to CRL X.509v2, following RFC 3280.

7.2.2 CRL and CRL entry extensions

Not defined.

7.3 OCSP Profile

The Online Certificate Status Protocol (OCSP) is used to validate the revocation status of all certificates signed by the Central Certification Authority. The use of OCSP is mandatory for all subordinate Certification Authorities. The OCSP responders must conform to RFC2560.

7.3.1 Version number

Version 1 of the OCSP specification as defined by RFC2560 is supported.

7.3.2 OCSP extensions

The OCSP service uses a secure timestamp and a maximum validity period of 5 minutes to verify the freshness of the signed response. The hash algorithm used for the issuer name and key is SHA1.

The nonce extension is supported by the OCSP responder. Requests containing a nonce should use it to verify the freshness of the response.

Otherwise, the local clock and the timestamp contained in the response should be used.

8 Compliance Audit and Other Assessments

AUTH PKI meets the technical specifications of ETSI TS 101 456 standard "*Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates*". An external CP/CPS compliance audit is required on a yearly basis.

A compliance audit may be conducted on demand by interested parties, provided there is appropriate permission by the institution which operates the Service 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. All kinds of exploitation or subcontracting of provided services from their recipients is expressly prohibited.

9.1.1 Certificate issuance or renewal fees

No fees are charged

9.1.2 Certificate access fees

No fees are charged

9.1.3 Revocation or status information access fees

No fees are charged

9.1.4 Fees for other services

No fees are charged

9.1.5 Refund policy

No fees are charged

9.2 Financial responsibility

AUTH PKI cannot undertake or pay damages for potential liability.

9.3 Confidentiality of business information

AUTH PKI does not handle commercial type of information.

9.4 Privacy of personal information

9.4.1 Privacy plan

Not defined.

9.4.2 Information treated as private

Private keys of the Certification Authorities, the source code and the private keys storage/operation procedures are considered classified and confidential information which are stored in the Certification and Registration Authorities. Information concerning the physical access and security of the premises where the Certification and Registration Authorities are installed and operated, is also considered classified.

It is likely that Registration Authorities undergo personal information processing during the identification procedure of the applicant.

9.4.3 Information not deemed private

Information included in the issued digital certificates is not considered private or confidential.

9.4.4 Responsibility to protect private information

All private and personal information handled and processed by AUTH PKI is in accordance with the Greek legislation concerning personal data protection.

9.4.5 Information disclosure to law enforcement and judicial agencies

All non classified information stored at the Certification and Registration Authorities is available to the law enforcement authorities, after their official written request. Classified and personal information can be disclosed to the judicial authority if there is an official court order according to the privacy and data protection applicable law. The process is carried out through the Rector's Office of AUTH. Private keys used to sign and issue digital certificates are

never disclosed to any third-parties, unless applicable law specifically demands disclosure.

9.4.6 Information disclosure available for entity queries

All non classified information stored at the Certification and Registration Authorities is available for entity queries, once applied for.

9.4.7 Conditions for information disclosure to its owner

All information stored at the CA and RA is available to its rightful owner (e.g. individual who applied for a certificate), once applied for.

9.4.8 Other information disclosure circumstances

Not defined.

9.5 Intellectual property rights

AUTH PKI does not hold any intellectual property rights on the issued certificates.

Anyone can copy parts of this CP/CPS with the condition that the original document is properly referenced.

9.6 Representations and warranties

Not defined

9.7 Disclaimers of warranties

Not defined

9.8 Limitations of liability

AUTH 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. Using AUTH PKI and its certification services requires that users unconditionally accept the terms and services of this CP/CPS and that AUTH PKI 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.

9.9 Indemnities

AUTH PKI cannot be held liable and does not undertake any financial, civil or other responsibilities unless there is evidence of fraudulent intent or serious negligence by its operators. AUTH PKI is strictly used for Academic and Research activities and cannot be used for commercial transactions. Therefore, AUTH PKI is exempt from any liability or damage that is not directly linked with the certification services for the already mentioned purposes.

9.10 Term and termination

This CP/CPS is valid and effective for as long as AUTH PKI is operational.

9.11 Individual notices and communications with participants

When a subordinate Certification Authority or Registration Authority decides to terminate their services and withdraw from AUTH PKI, it is obliged to officially inform the Administration of Certification Service. Similar correspondence is essential when Academic or Administration units of AUTH wish to participate and become a member of AUTH PKI.

9.12 Amendments

9.12.1 Procedure for amendment

Syntax changes can be made to the Certification Policy and to the Certification Practice Statement without any prior notice and without OID modification.

9.12.2 Notification mechanism and period

There will be prior notification to subscribers in case of major changes to the CP/CPS. AUTH PKI is obligated to publish (at its web site), previous versions of its CP/CPS in case of major document changes. The most recent CP/CPS is always published at the following URL: http://www.pki.auth.gr/documents/CPS.php.

9.12.3 Circumstances under which OID must be changed

In case of major and significant changes of the CP/CPS, the name and identifier (OID) which is reported in section 0 will be altered.

9.13 Dispute resolution provisions

Differences or disputes that result from the interpretation of the 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 the courts of Thessaloniki that are competent.

9.14 Governing law

AUTH PKI is focused on serving the Academic Community of AUTH. 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 AUTH PKI unless otherwise specified in a subCA with a separate CP/CPS. The operation of the AUTH 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 issued 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 issued can be used as 'qualified'- like these that are defined at the Presidential Decree 150/2001- in closed teams of entities, as for example in certain administrative units of AUTH. These procedures must be described on a separate Certification Policy/Certificate Practice Statement (CP/CPS) document that corresponds 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 1.3.3, the CP/CPS document must not conflict with any condition of the present document. Basic conditions for this "qualification" and accordingly the "qualification" of the 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).

9.15 Compliance with applicable law

AUTH PKI is completely abided by the Greek Legislation.

9.16 Miscellaneous Provisions

9.16.1 Certification Authority Obligations

A Certification Authority is responsible for the issuance and the management of the certificates. Specifically AUTH certification authorities are bound to:

- ✓ Provide and maintain the infrastructure that is required for constitution of hierarchy of certification services for the Aristotle University of Thessaloniki, according to the certification processes described in this document.
- ✓ Implement and maintain the security requirements according to relative sections of the present document
- ✓ Accept or reject requests for certificate issuance according to the relative sections of the present document.
- ✓ Maintain a publicly accessible directory for certificates and CRLs. This information should be publicly available via widely used protocols such as HTTP, FTP and LDAP.
- ✓ Revoke certificates when specific reasons apply or after a proper request by the subject of the certificate.
- ✓ Maintain the CRLs up to date.
- ✓ Manage all personal and private information of the subscribers with confidentiality.
- ✓ Immediately inform the technical personnel of Subordinate CAs for any loss, exposure, modification or unauthorized usage of the CA's private key.

- ✓ Ensure that all the services provided within the whole infrastructure, abide by the terms and conditions of the present CP/CPS.

9.16.2 Responsibilities of subordinate Certification Authorities

Each subordinate Certification Authority approved by AUTH PKI is committed to:

- ✓ Grant certificates with validity period within the limits of the active employment (or other) relationship between the applicant and the unit she/he is involved, according to the applicant's affiliation (i.e student, employee. etc).
- ✓ Inform the Central Certification Authority of AUTH immediately in case of private key exposure.
- ✓ Protect the private keys, used for certificate signing, at least in the security level that is described in the present document.
- ✓ Develop (optionally) its own policies and procedures of certification which must be at least as strict and binding as the ones described in the present document.

9.16.3 Registration Authorities Obligations

Each Registration Authority manages the applications for subscriber registration.

- ✓ Each Registration Authority is responsible to receive certificate applications from subscribers. It validates the identity of the subscriber, confirms that the public key that is submitted belongs to the subscriber and securely transmits the application to the CA.
- ✓ According to the certificate type, applications can be submitted via face-to-face meeting with the interested party, via e-mail, via a secure web form, or via any mechanism that securely identifies the user. The application includes all information identifying the subscriber, and the corresponding public key.
- ✓ Mass applications submission from a specific administrative unit is possible on behalf of the persons that belong to that unit

- ✓ Each Registration Authority must verify if each person requesting a personal certificate is the rightful owner of the certified e-mail address.
- ✓ Each Registration Authority must verify that the person requesting a device certificate is the rightful owner and administrator of the device's FQDN.

9.16.4 Subscribers Obligations

- ✓ AUTH PKI subscribers are obligated to read, accept and comply with this Certificate Policy/Certification Practice Statement. Subscribers are obliged to use the certificates only for the purposes described in this CP/CPS and the applicable law.
- ✓ Subscribers must create a key pair (private and public) using a reliable and secure system and take all necessary precautions to protect their private key from accidental destruction, loss or theft.
- ✓ After the subscribers receive their certificate, they agree and confirm that the information contained in the certificates is accurate.
- ✓ Subscribers must request certificate revocation when it is not used anymore, when the data contained has changed or when it is suspected that the private key has been compromised or lost.
- ✓ Especially in case of code signing, subscribers are bound by the RA to provide complete, accurate and truthful information (eg, application name, information URL,application description, etc.) in the signed code.

9.16.5 Relying party obligations

- ✓ Entities that trust the issued certificates are obligated to read and accept this Certificate Policy/Certification Practice Statement and to use the certificates only in ways that conform to this CP/CPS and the current legislation.
- ✓ Entities that trust the certificates must check the validity of the digital certificate signature and trust the parent Certification Authorities. Finally, they should periodically check the validity of the certificate against the relevant Certificate Revocation List of use the

Online Certificate Status Protocol (OCSP) service for possible revocations.

9.16.6 Repository obligations

Each Certification Authority (Central or Subordinate) is obligated to operate and maintain a publicly accessible data repository containing:

- ✓ the certification authority certificate
- ✓ the Certificate Policy/Certification Practice Statement
- ✓ the subordinate Certification Practice Statements
- ✓ the issued certificates
- ✓ the Certificate Revocation Lists