DIGITAL CERTIFICATION SERVICES

CERTIFICATION PRACTICE STATEMENT OF NON-QUALIFIED CERTIFICATES

(CERTIFICATION PRACTICE STATEMENT OF NON-QUALIFIED CERTIFICATES)

Version 1.1 - 15/03/2016

OID: 1.3.6.1.4.1.29402.1.2.1.1

Approved for the following ATHEX "Certificate Policies":
(Approved for the following 'Certificate Policies':)

1. Server Authentication Certificate Policy 'Trust-Server -Class 1'
   (1. Server Authentication Certificate Policy 'Trust-Server -Class 1')
   OID: 1.3.6.1.4.1.29402.1.2.1,1

2. Certificate Policy for Non-Qualified Certificates 'Smart-Sign -Class 1'
   (2. Certificate Policy for Non-Qualified Certificates 'Smart-Sign -Class 1')
   OID: 1.3.6.1.4.1.29402.1.2.1.1

{deliberately empty}

- CONTENTS -

PART I: INTRODUCTION

1.1 GENERAL INFORMATION

1.1.1 PRESENTATION OF ATHEX S.A. AS A CERTIFICATION SERVICE PROVIDER (C.S.P.)

1.1.1.1 Incorporation, purpose and activities of ATHEX S.A.

ATHEX S.A. belongs to the group **"HELLENIC EXCHANGES S.A. (HELEX) HOLDING"** (http://www.athexgroup.gr).

Along with the financial activities, ATHEX develops software products that help in the better organization, management and data support of other HCMC players, such as members of ATHEX'S Securities Market and Derivatives Market, listed companies, financial institutions and investors.

Some of the projects that ATHEX successfully designed developed or administers include:

- the **"Integrated Automated Electronic Trading System (OASIS)"** and ATHEX'S **"Securities Trading Network (STN)"** through which securities are traded in the Hellenic Capital Market Commission's Share, Bonds and Derivatives markets on a daily basis,
- ATHEX'S **"Statistics and Reporting System (SRS)"** on which ATHEX bases the operation of its data dissemination services,
- the HELEX websites (www.athexgroup.gr),
- ATHEX'S **MarketSuite** application suite that addresses securities firms and investors.

1.1.1.2 ATHEX'S 'Digital Certification Services'

Given the growing need for security in electronic communications, especially in areas such as the HCMC, ATHEX was compelled to create an independently functional operational unit, entitled "**Digital Certification Services**", which assumed the development, implementation and support of a **modern and reliable electronic trading security system** with the use of '**advanced electronic signatures**'.

As part of this section, ATHEX

- **utilized** the experience, expertise and reliability of its personnel,
- **using** the latest - both in software and hardware - technological applications for this purpose,
- **taking advantage** of the potential and the institutional framework established by the European Directive 99/93 'for electronic signatures' and adaptation of the corresponding Greek p.d. 150/2001,

it developed a **modern and reliable** '*Public Key Infrastructure*'(*PKI*) for the **provision** of "**trusted services" to the public** (as a 'Trusted Third Entity') involving the issuance and management *of **electronic certificates***' and the creation of '**advanced electronic signatures**', both from natural persons and from devices or software involved in an online communication.

1.1.2 OPERATION OF ELECTRONIC SIGNATURES, INSTITUTIONAL FRAMEWORK & APPLICATIONS

Note: List of References, Definitions and Abbreviations, as well as 'Frequently Asked Questions (FAQs) & Answers' to better understand the operation of ATHEX'S electronic signatures and certificates which are provided in ATHEX'S Repository (see. paragraph 2.3.1).

1.1.2.1 Cryptography of Asymmetric Keys and Trusted Path of Public-Keys

The entire operation of the electronic signatures is based on the modern cryptographic system that uses "**asymmetric keys**" (unique pairs of keys) each of which has the capacity of decrypting only what has been encrypted by another - unique - key, without it being simultaneously possible (with modern technology) to extract (or rebuild) one key from another.

Thus, keeping one key secret (private) and disclosing the other key (as public) we ensure that only we can encrypt something that everyone else (those who know our public key) can decrypt (in fact, with the certainty that it comes from us), while everyone can (with our public key) encrypt something, knowing that only we (who possess the corresponding -unique- private key) can decrypt and read it!

Although the above technology ensures that we can disclose our public key to anyone without jeopardizing the security of the encryption, the need arises, especially when we want to use the key pair in a wide range of applications with multiple or even unknown recipients, for the existence of a **'Trusted Third Entity'** which will confirm and certify to any third party/recipient of our public key, **both** our true identity, **and** that fact that we actually possess the private key that corresponds to the disclosed public key.

In order for this 'entity' (usually called the 'Certification Services Provider - CSP), to generate confidence to everyone, it should organize a **reliable**, both in terms of technology and procedures, '**Public Key Infrastructure' (PKI)**, which will be documented with very clear and publicized terms and procedures, under which it will issue, after proper control, standard **'electronic certificates**' for correlation of a person or an object with a certain 'public key', which will be **readily available for verification** by every remote third party.

The fact that the 'electronic certificates' themselves must, in turn, bear the 'electronic signature' (accompanied by the relevant 'public key') of the CSP that issues them, requiring a **new unique certificate** (so as to preclude forgery of certificate), leads to a sequence of certificates which ends with the existence of a 'self-signed certificate'. This certificate, which is also the top of the pyramid of a 'PKI' Infrastructure, is issued by the '**Root Certification Authority**' 'or 'Root CA', who apart from this certificate for its own keys - usually signs certificates for the keys of 'lower' ranking '**Certification Authorities**' or 'CAs' or Subordinate CAs or Sub-CAs, who also undertake to issue and sign certificates for '**end entities**' (persons or subjects that have certified cryptographic keys).

The public key certificate path that links the original certificate by the "Root Certification Authority" (thus transferring its credibility through the successive certifications) to the 'end entity' certificate (also the certificate's 'starting point'), is called the ***Trusted Path*** and constitutes the basis for the electronic certification services' operation with the use of public keys.

1.1.2.2 Applications of electronic signatures and certificates

The various applications that use electronic signatures and electronic certificates are summarized in the following sections:

a) The **signing of an 'electronic document'** by a natural person with the use of a 'qualified certificate' and 'Secure Signature Creation Device' *(e.g. smart card)*, in order to ensure, other than the signatory's authenticity and the integrity of the signed document, the signatory's legal obligation (*Non-Repudiation*) regarding the content of the document, such as the handwritten signature on a 'paper' document (see below for the institutional framework)

b) The **signing of 'emails'**, which requires the signatory's email address to be certified by the CSP, thus ensuring the sender's authenticity (that the signatory is actually the sender) and integrity of the signed message (that it has not been altered by a third party) to the recipient

c) The **assurance of a person or device's identity** during their communication (*replacing the 'User Name' and 'Password'*), thus offering different access levels to a web site or an online service on an individual basis. Other than the subject's identity, it is also possible to certify various 'attributes' in the electronic certificate, so that access to the application is controlled on a group basis, depending on the attribute.

d) The **encryption of 'documents' and 'sent messages'** by using the public key of a subject, thus ensuring that only the holder of the corresponding private key (recipient or even the cryptographer himself if he uses his own public key) can decrypt and read the document or message.

1.1.2.3 Institutional framework and electronic signature categories

With the dissemination of advanced electronic signature technologies and after many preparatory processes and consultations, in December 1999 the European Union issued directive [EC 99/93] 'on a Community Framework for Electronic Signatures', which was adopted in Greece with [p.d. 150/01] (Official Gazette, issue A -125/25.6.01). According to this p.d. (art. 3 §1): *"the **advanced electronic signature** which is based on a **qualified certificate** and is generated **by a secure signature creation device** serves as a handwritten signature both substantive and procedural law*'. (analysis of the above definitions see chapter 6.2 of the Practice Statement's Annexes).

The contribution of all the above terms in one electronic signature (which we will hereinafter refer to as **'qualified electronic signature'**) OBLIGES law enforcers to consider the specific electronic signature as handwritten; however, this does mean that other electronic signature categories that do not fully meet all the above requirements are deprived of every status.

Respectively, the next paragraph of the same p.d. (art. 3 §2) defines that "*The validity of the electronic signature or the admissibility as evidence is **not excluded** for the simple reason that it does not meet the conditions of the previous paragraph*" thus setting another electronic signature category (which we will later refer to as **'non-qualified electronic signatures'**) for which additional evidence may be required for the affirmation of the validity of such an electronic signature.

A particularity of **European legislation** for electronic signatures is the institutionalization of a particular type of 'qualified certificates' which - under additional requirements - create 'qualified signatures'. Therefore, if a certificate could theoretically be used for all the above applications (*which is often encountered in practice by many certification authorities whose focus is not on supplying 'qualified' certificates such as ATHEX*), **security reasons (key management by the operator, non-waiver of liability (non-repudiation), responsibility and accountability) and reliability demand** [CWA 14167-1, KM3.4], **the certificate** (and corresponding key pair) **that is intended for the creation and verification of a "qualified electronic signature" shall not to be simultaneously intended for other applications**.

Therefore, it is deemed proper to provide natural persons as well as the legal representatives of legal entities, according to circumstance, with **two different certificates**, namely a 'qualified' certificate for the creation of a natural person's 'qualified digital signature' (which is legally binding - see Certification Practice Statement of Qualified Certificates OID 1.3.6.1.4.1.29402.1.1.1.1) and one or more certificates for other uses, such as for 'verifying the identification' of that person in controlled access applications (e.g. web sites), for the use of "secure email" and/or data "encryption and decryption".

1.1.3 NATURE AND STRUCTURE OF THE PRACTICE STATEMENT

1.1.3.1 Purpose of this documentation

The documentation of ATHEX'S "Digital Certification Services" (hereinafter "ATHEX"), entitled '***Certification Practice Statement of Non Qualified Certificates** ('CPS- Non-QC'),* is intended **to analytically identify, record, and to disclose to every party** (*and its partners, subscribers and third-parties that are dependent on its services; principles and related verification and/or accreditation bodies*) **the terms and conditions and (if conditions are translated) it may be better to refer to conditions and requirements as well as operational and business practices** that are applied or govern the provision of ATHEX'S Digital Certification Services, and specifically the Policy and Certification Practice Statement for Non-Qualified Certificates.

The '**Policy for Non-Qualified Certificates**' that is issued by ATHEX'S '*Policy Management Committee*' (see below -Paragraph 1.2.5), identifies and analyzes the terms of issuance, management and use for the Non-Qualified Certificates issued by ATHEX.

This text (the "**Certification Practice Statement**') for Non-Qualified Certificates determines the organization of its services, the general operating principles and practices applied and the security measures

taken during the provision of ATHEX'S certification services for the Non-Qualified Certificates in question. (*Note: All supported certificate Policies and the present Practice Statement are published by ATHEX in its 'repository' - see paragraph2.3.1*)

Thus, after reading this "Certification Practice Statement" and the related "Certificate Policy", every interested individual is able to assess and evaluate the degree of security and reliability offered by the specific type or group of certificates issued by ATHEX, **so as to decide on their own if they will rely on the information provided therein and/or for their appropriateness in relation to the purpose or application that they are intended for.**

Finally, this document intends on simultaneously providing the reader (in relation to the publications in the ATHEX repository) with **general education** and **a fundamental basis with information and referrals to relevant sources or texts** for the definition, use and legal consequences of the advanced electronic signatures.

1.1.3.2 Structure and content

This "X.A. Certification Practice Statement of Non-Qualified Certificates' *or 'X.A. CPS of Non-QC'*) is based on the 'standard' [RFC 2527] and takes into consideration the requirements of the 'standard' [TS 101 456, v1.2.1].

The structure of this Practice Statement differs from the structure proposed in standard [RFC 2527] to the extent that is necessary to properly describe and simplify the understanding of the operational practices followed under ATHEX'S 'Digital Certification Services'.

The Practice text is divided into **five (5) Parts**:

PART I: **INTRODUCTION**	*general information about ATHEX; introduction to the PKI and the institutional framework; identification of this documentation; presentation of the structure of ATHEX'S services; description and applications of ATHEX'S certificates; contact details.*
PART II: **GENERAL TERMS AND POLICIES**	*Obligations and responsibilities of the parties involved; ATHEX'S guarantees, disclaimers and limitations of liability; and policies regarding personal data protection, the resolution of disputes, the provision of information, archiving, the pricing policy, etc.*
PART III: **OPERATING TERMS**	*Certificate Application; identification of the applicant; creation of keys and customization of their device; certificate issue; certificate expiration, renewal and creation of new keys; cessation and revocation of certificates; key change; termination of services*
PART IV: **SYSTEM RELIABILITY & CONTROL**	*Technical security standards, such as the creation and protection of ATHEX keys; security network, etc., and physical security specifications; control and security of procedures and data for reliability and personnel training*
PART V: **DESCRIPTION OF CERTIFICATES & CRLs**	*Structure and contents of X.509 v.3 certificates and of "Certificate Revocation List" (CRL); naming rules, fields used and their extensions, meaning and interpretation of the fields contents, field criticality, etc.*

1.1.3.3 Version Number and Revisions of part or all of the Practice

This Practice is characterized by a **'version date'** and a **'version number'** consisting of two figures separated by a dot (.) the first of which indicates the number of revisions made to the Practice, while the second, the secondary and/or minor changes to individual documentation areas. The first approved version is numbered with the code '**1.0**'

Revisions to part or all of this Practice Statement may be made periodically, or whenever deemed necessary by ATHEX. These revisions are published and enforced in accordance with the provisions of paragraph 2.3.4.

Every new or amended version of the Practice Statement receives a new 'version number' by increasing the first or the second digit, depending on the criticality of the change.

(*Note: Additions to Part VI of this Practice (Annexes), which are intended to assist the reader in understanding the function and regulatory framework of electronic signatures, may be made at any time without change of the 'version number' and no other publication obligations*.)

1.1.3.4 Identification Feature (OID) of this Practice

This document must be abbreviated as "X.A. **C.P.S.- N.Q.C. ver. 1.0"**

The globally unique identifier (OID) of this document is:

1.3.6.1.4.1.29402.1.2.1.1

where:

1.3.6.1.4.1.29402	***ATHEX Identifier (OID), registered by the IANA***
1	***ATHEX'S Independent "Public Certification Services" department***
2	***Certification Practice Statement of Non- Qualified Certificates***
1.1	***First and second digit of the Practice's version number***

1.2 DESCRIPTION AND STRUCTURE OF ATHEX'S 'DIGITAL CERTIFICATION SERVICES'

Note- Clarification: All references to certificates and related services in the document relate to Non-Qualified Certificates and related services, unless otherwise explicitly stated. Furthermore, any reference to the Certification Practice Statement and Certificate Policy concerns Certification Practice Statement of Non- Qualified Certificates and the Policy of Non- Qualified Certificates

1.2.1 OPERATIONAL DISTINCTION OF OFFERED SERVICES

The services provided by ATHEX as a 'Third Trusted Entity' to the public as part of its 'Digital Certification Services' are operationally divided into the following distinct 'operational entities':

1.2.1.1 Registration Service

The '*Registration Service',* which is also referred to as '*Registration Authority'* or *'RA'*, accepts the applications that are submitted by candidate subscribers (certification subjects) from the collaborating '*Local RA Assistants'* (*see paragraphs 1.2.1.7 and 1.2.3.2*) and once the applicant's identity and public keys are verified, it authorizes the issue of certificates and forwards the subscriber's accurate details to the '*Certificate Generation Service'*.

1.2.1.2 Certificate Generation Service

The '*Certificate Generation Service'*, having individual '*Operational Certification Authorities*' ('*Operational CAs*') or Subordinate CAs (Sub-CAs) for each certificate type or class, creates, issues and signs certificates based on the identity and other information that has been verified and transmitted by the '*Registration Service'*. For this purpose, the service's 'Certification Authorities' who sign the end entities' certificates, have different cryptographic keys, certified by the 'X.A. Root CA'. In addition, the Subscriber is able to use the specially-designed web application for the generation, renewal or revocation of his certificates. Also, via this application he securely creates asymmetric cryptographic key pairs.

1.2.1.3 Subscriber Device Provision Service

The *Subscriber Device Provision Service*, if provided by the requested certificate policy, securely creates asymmetric cryptographic key pairs for subscribers, which it transfers to a 'customized' signature creation device for these entities (e.g. smart-cards). The Service supplies the subscribers with these devices

and at the same time informs the '*Registration Service'* of the subscriber's generated public keys that require certification.

1.2.1.4 Dissemination Service - 'Repository'

The *Dissemination Service*, via ATHEX'S *'Repository'* - which maintains and updates- (see paragraph 2.3.1) disseminates and distributes all the terms and conditions for the issuance, management and use of certificates to every subscriber or third party (e.g. this 'Certification Practice Statement of Non-Qualified Certificates', the 'Non-Qualified Certificate Policy', etc.) as well as the list with the current and revoked (or ceased) certificates.

1.2.1.5 Revocation Management & Status Service

The *Revocation Management & Status Service* handles the applications and reports for the suspension or revocation of certificates and decides on the necessary actions. It issues updated "Certificate Revocation Lists" (CRLs) on an ordinary and/or extraordinary basis, which are signed by the same 'Operating Certificate Authority' that issued and published them in cooperation with the '*Dissemination Service'*.

1.2.1.6 Time-Stamping Service

The '*Time-stamping Service'* provides time stamped certificates for electronic documents at the request of 'bearer' of the document. This service significantly contributes to the long-term verification of electronically-signed documents.

1.2.1.7 Local RA Assistants

The '*Local RA Assistants*', who cooperate with ATHEX'S Digital Certification Services, assist prospective subscribers with their application for certificates by providing them with the necessary printed material (applications, contracts, documentation, etc.) and providing them with billing services. The Local RA Assistants cosign the subscribers' applications - following a quick perusal of their supporting documents; and forward them to the competent '*Registration Service*' for approval. On occasion, and in cooperation with the relevant '*Subscriber Device Provision Service*' they provide to prospective subscribers with suitable 'Secure Signature Creation Devices'.

1.2.2 THE ATHEX COMMITTEES

Apart from the above operational entities that perform the individual certification services, the following Committees operate within the framework of ATHEX'S Digital Certification Services:

1.2.2.1 'Policy Management Committee' (PMC)

The PMC is composed of ATHEX'S senior executives with the participation of experienced / specialized technical and legal advisers and constitutes the body that is responsible for policy making and designing the digital certification services offered by ATHEX.

Once the PMC takes into consideration the technological developments, the regulatory framework, the trade and transactional requirements (of ATHEX and/or subscribers and ATHEX'S business plans, it issues and/or amends the **'Non-Qualified Certificate Policies'** *(which define the terms of issue, management and use for all types of electronic certificates issued by ATHEX with the exception of the Qualified Certificates)*, and approves ATHEX'S current '***Certificate Practice Statement of Non-Qualified Certificates'*** (and possibly other Certificate Service Providers) or their revisions, ascertaining its appropriateness in support and execution of the above Policies.

The PMC meets regularly once a month to examine the current conditions and the need to revise or issue new Certificate Policies, to adopt new or amended Certification Practice Statements, and to genuinely interpret the provisions of its Policies where a relevant query is raised.

1.2.2.2 'Complaint Handling and Dispute Resolution Committee' (CHDRC)

The CHDRC meets regularly once a month and extraordinarily whenever deemed necessary by circumstances, with the competency of checking compliance of the Certification Practice Statement and the handling of any complaints and/or the resolution of any differences related to ATHEX'S Digital

Certification Services.

It consists of ATHEX'S executives and specialized technical and legal advisers who carry out procedures that are provided in Chapter 2.7 ('Dispute Resolution Policy') and forwards queries to ATHEX'S PMC when in doubt.

The CHDRC has full access to the records and logs of ATHEX'S Digital Certification Services and prepares an annual report addressed to the PMC with its activities and conclusions on an annual basis.

1.2.3 CERTIFICATE COMMUNITY AND CONTRACTING PARTIES

1.2.3.1 ATHEX as the 'Certification Service Provider'

As a 'Certification Service Provider' ATHEX **contracts either directly** (with their own Local RA Assistants) **or indirectly** (through collaborating Local RA Assistants operating from authorized third parties - see below) **with its subscribers** in order to issue and manage electronic certificates for them and their devices.

Based on the high security standards laid down in this Certification Practice Statement, as a **'Root CA'**, ATHEX creates the basic cryptographic key pair with which it issues and signs its certificate (self-signing) and the certificates of all its **'Subordinate CAs'** that issue certificates to end entities, thereby establishing an integrated 'public key infrastructure' (PKI), which supports the services it provides.

ATHEX may assign part or all of the services stated in paragraph 1.2.1 to collaborating third parties (natural parties or legal entities) thereby creating a '**X.A. Public Certification Services Network**' (hereinafter the "Network"); however, it retains **total liability** towards its subscribers and users of its certificates. The members of the 'Network' undertake to provide to their subscribers and third parties the services that they have been assigned (e.g. Registration Service, Issue Service, Dissemination Service, etc) in accordance with the terms of this Practice Statement, **being responsible according to existing cooperation agreements towards X.A. and being under its direct control** concerning compliance with the above terms.

1.2.3.2 Local RA Assistants

The Local RA Assistants are usually **independent organizations or companies** that collaborate with ATHEX (or an authorized member of its 'Network' that provides "Registration Services") in order to contribute in the provision of ATHEX'S services to associated (as employees, customers or partners) persons or entities (e.g. servers), possibly for sharing ATHEX'S certificates in a specific application. Although the Local RA Assistants do not provide 'Registration Services' they constitute the **exclusive channel** for a subscriber to apply for registration and to obtain certificates from ATHEX.

Thus, the Local RA Assistants **undertake** the update, the supply of appropriate printed material and the billing of the certification services to the public, which they address. The Local RA Assistants can also provide (either mandatorily or optionally and at their discretion) their own "secure signature creation devices' (e.g. smart card) to subscribers that join ATHEX through them, which is customized (by way of personal data) for subscribers of the network's *'Subscriber Device Provision Service*'.

Through authorized agents which they designate as '*Local RA Assistant Administrators*', the Local RA Assistants mandatorily **cosign** the candidate subscribers' 'Certification Application and Subscriber Agreement', which they forward (along with the other necessary documents) to the network's competent Registration Service. Finally, the Local RA Assistants **charge** the applicants with all the fees and costs relating to the services provided by the ATHEX network having an independent 'Pricing Policy'.

Local Submission Service may be operated by ATHEX'S legal entity for certification needs of its existing technological infrastructure.

1.2.3.3 Subscribers

Subscribers or those certified by ATHEX are either natural persons to whom one or more personal certificates have been issued, or legal entities for which a certificate has been issued for an object or device (e.g. server) of their ownership from ATHEX'S Digital Certification Services Network.

To become a 'subscriber' the party must address a 'Local RA Assistant' of the ATHEX network in order to complete the relevant Application -simultaneously submitting the necessary supporting documents - and to sign the 'Subscriber Agreement'. If the application is **approved** by the competent Registration Service (RS) of the ATHEX network, it then instructs the network's relevant Operating Certificate Issuer, who issues the certificate.

1.2.3.4 Certificate Users ('Relaying Parties')

Certificate users or relaying parties are the natural persons or legal entities who, further to being informed and agreeing with the terms and conditions of use of the certificate that are included in this Practice Statement, in the relevant 'Certificate Policy' and 'User/Recipient Agreement', and after checking and verifying the validity of a certificate that has been issued by the ATHEX network according to the above (either by the supervisory process or the use of automated applications) **decide for themselves** whether to rely on the contents of the certificate or not, so as to carry out a particular transaction, action or omission, or to acquire the legitimate expectation for an event.

A 'Certificate User' may well be a subscriber or even a member of the ATHEX network itself, who, by following the above procedure, relies on the certificate of a third party issued by ATHEX or not.

1.2.4 CERTIFICATE TYPES & APPLICATIONS ISSUED BY ATHEX

1.2.4.1 Certificates for Natural Persons

For natural persons, ATHEX issues the **"Smart-Sign™"** Personal Certificates 'Pack' which simultaneously comprises of **two complementary certificates (**which correspond to two different pairs of asymmetric cryptographic keys), namely:

1) The '**Qualified Personal Certificate**'(QPP), intended exclusively for the certification of digital signatures that are legally equivalent to handwritten signatures and
2) The '**Personal Identification Certificate**'(PIC)
   I. for verification of a person's identity for use as a medium of limited (customized) access to telematic applications, for signing emails and for secure communications between persons or via servers.
   II. Encryption and decryption of other - usually temporary - symmetric encryption keys *(used for direct secure communication between the two systems)*
   III. Encryption and decryption of personal files and data (data encryption)
   IV. Financial transactions, i.e. transactions involving the provision or exchange of goods (tangible or intangible) or services (that bring about changes in the asset/financial situation of the transacting parties), regardless of whether they involve monetary transactions
   V. Code Signing, for 'signing' files that directly or indirectly constitute a direct or indirect executable code for PCs **(**'software', e.g. files with extensions .exe or .com) or add ons to an existing executable code that bring about different possibilities to a PC (e.g. .dll extensions).

These certificates are divided into **classes** (e.g. Class 1, Class 2 and so on) of which each corresponds to a unique Certificate Policy (approved by ATHEX'S 'Policy Management Committee') with differences mainly in the certificates' limitation of the use, the value limits of permissible transactions and the maximum liability level that ATHEX undertakes for each certificate class and their pricing.

In accordance with the Policy provisions, a Smart-Sign™ personal certificates pack **always** consists of certificates of the **same class** and they are always stored in **the same** customized device**.**

1.2.4.2 Certificates for Devices

ATHEX also issues certificates for devices, such as 'servers ('**Trust-Server™' Certificates**), which belong to a natural person or legal entity that is treated as the "Subscriber" of that certificate.

These certificates correspond in their operation with 'personal identification certificates' by providing secure communication of these devices with others, using **high 1024bit SSL type encryption**. Certificates for devices issued by ATHEX are also distinguished into **classes**, but have a different 'application-subscription contract', different authentication process' and 'key pair verification', and, of course, a different 'Certificate Policy', which defines these processes.

1.2.4.3 Certificates for Certificate Authorities (or 'Certificates CA')

Apart from the above types of certificates that are intended for end entities, ATHEX (as a Root CA) also issues certificates for its network's 'Certification Authorities' (CAs), which are solely intended to certify their signatures and to respectively authorize their Subordinate CAs for issuing certain certificate types and classes to end entities.

Such certificates (also referred to as 'CA Certificates') have naturally been issued for all ATHEX'S 'Subordinate CAs', while the issuance of such certificates to third (authorized)' Certification Authorities' **requires a specific contract** between ATHEX as the Root CA and certification authorities, a component of the **present** ATHEX Practice Statement and reference will be made to specific 'Certificate Policies' that can be issued by authorized CA.

1.2.4.4 More About Certificates Types

For more information about the utility, destination, content, the specific terms and conditions of use of each certificate, please refer to the corresponding '**Certificates Policies**' which are available online (except the 'CA certificates' policy) in ATHEX'S 'Repository' (on the website www.athexgroup.gr/web/guest/digital-certificates) or contact ATHEX (See contact information below) or a Local RA Assistant for more information and printed versions of the texts.

1.2.5 CONTACT DETAILS

Communication and any notifications to ATHEX'S DCS, its network's of services, or the above Committees, must be made to the address:

ATHENS STOCK EXCHANGE

DIGITAL CERTIFICATION SERVICES

110 Athinon Ave., 10442

Athens

Tel.: +30 210 336 6300

Fax: +30 210 336 6301

e-mail: PKICA-Services@athexgroup.gr

web: http://www.athexgroup.gr/el/digital-certificates

PART II: GENERAL TERMS AND POLICIES

2.1 OBLIGATIONS

2.1.1 OBLIGATIONS OF THE CERTIFICATION SERVICES PROVIDER

2.1.1.1 ATHEX'S obligations as the 'Root Certification Authority'

As the 'Root Certification Authority' ('RCA' or 'Root CA') and founder of its "public key infrastructure" (PKI), ATHEX has the following obligations:

1) To support the operation of the 'Public Key Infrastructure' (*PKI*) and to make every reasonable effort to maintain a reliable system in accordance with the provisions of this Practice Statement.

3) To publish and disseminate the 'self-signed certificate' and 'CA Certificates' of the 'Operational Certificate Authorities' (*Operational CAs*) that it has issued.

3) To adopt and approve, through its Committees, the Certification Practice Statement, Policies for each type, kind or class of certificate that is issued by its network and, generally, all the conditions governing the provision of its 'digital certification services'.

4) To supervise, conduct regular controls and to support all operational entities within its network (RS, CGS, RMSS, Local RA Assistants, etc) so that they comply with the terms and conditions set out in this Certification Practice Statement.

2.1.1.2 Obligations of the Registration Service

ATHEX'S 'Registration Service' (RS) and every contracted RS in ATHEX'S network, has the following obligations:

1) To examine the subscribers' applications that it receives from cooperating '*Local RA Assistants'* and to proceed with their approval **no later than five (5) working days** of their receipt provided they meet the terms and conditions set out in the Practice Statement and in the Policy of the relevant certificate.

2) To confirm or ensure - with the collaboration of '*Subscriber Device Provision Service*'- that the certified subscriber possesses 'signature creation data' (private keys) (*Proof of Possession*).

3) To give the relevant mandate to '*Certificate Generation Service*' for generation of the relevant certificate, providing the complete and accurate information for the data to be included in the certificate.

4) To cooperate with the '*Revocation Management & Status Service*' for the required verification of the subscriber's identity during application for cessation, revocation or activation of its certificates.

5) To maintain a file with the subscribers' applications, contracts and supporting documents for which it approved the generation of certificates for the period specified in the Practice Statement and Policy of each certificate *(see Chapter 2.6 "Data Archiving Policy')*.

2.1.1.3 Obligations of the Certificate Generation Service

As part of its 'Certificate Generation Service' (CGS), ATHEX as well as every CGS in its network assumes the following obligations by issuing certificates to 'end entities':

1) To issue certificates in compliance with this Certification Practice Statement and relevant certificates Policy, and the certificates are to include the exact data that was examined and approved by the cooperating '*Registration Services*'.

2) To publish a list of generated certificates in ATHEX'S '*repository*' (via the collaborating *'Dissemination Service'*), and to cooperate with the relevant *'Subscriber Device Provision Service*' for the registration of these certificates in the subscriber's 'secure signature creation device'.

3) To sign the published 'Certificate Revocation Lists' ('CRL') relating to certificates that is generated, as reflected by the respective '*Revocation Management & Status Service*'.

4) To check its records for the generation of a previous certificate with the same signature verification data (towards the same or another entity), thus prevents double certification of own keys in its environment.

5) To electronically record and archive an exact journal of all important movements involving every certificate that it generates (issue, cessation, reinstatement, revocation, etc.) for the period specified in the Practice Statement and the Policy of every certificate *(see Chapter 2.6 "Data Archiving Policy')*.

2.1.1.4 Obligations of the 'Subscriber Device Provision Service'

The ATHEX network's 'Subscriber Device Provision Service' (SDPS) has the following obligations:

1) To create electronic signature creation and verification data (private and public key pairs) and to save them in the subscribers' customized "secure signature creation device" ('SSCD'), pursuant to recognized legal, technical and business models, collaborating with the relevant '*Local RA Assistants*' to supply these authorities.

2) To forward the created public key that will be certified for the subscriber to the *'Registration Service'* and to store the relevant electronic certificate that they receive from the '*Certificate Generation Service*' in the customized device, provided it is generated.

3) to observe every procedure that is provided by the Practice Statement and the relevant Certificate Policies for non-disclosure and non-replication of the subscriber's private key as well as for the safe transfer of the device and the activation code to the latter.

2.1.1.5 Obligations of the Dissemination Service - 'Repository'

Via the 'Repository, the 'Dissemination Service' (DS) of the ATHEX network (*see paragraph 2.3.1*), has the following obligations:

1) To promptly publish all applicable documentation relating to ATHEX'S "Digital Certification Services' (such as Certification Practice Statement, Certification Policies, Contracts, etc), as well as any previous important versions of these texts.

2) To publish and provide the downloading of all 'CA certificates' in the ATHEX network by anyone (*the basic certificate by the ATHEX'S Root CA and the certificates of all the network's 'Operating Certification Authorities'*) that are necessary for the formation of the '*Trusted Path'* that confirms the authenticity of the certificates of the network's end entities (subscribers).

3) To provide *links*, through the pages of the 'Repository', to the public Directories of the network's generated certificates and the '*Certificate Revocation Lists*' ('CRLs') concerning these certificates.

2.1.1.6 Obligations of the Revocation Management & Status Service

The 'Revocation Management & Status Service' (RMSS), which operates within the framework of ATHEX'S network, has the following obligations:

1) To maintain the ongoing operation of the electronic *Directories* with updated '*Certificate Revocation Lists'* ('*CRLs*') which bear the electronic signature of the '*Operational CA'* of the collaborating CGS that revoked (or ceased) certificates that are referred to them.

2) To cooperate with the '*Registration Service*' for the required verification of the subscriber's identity during application for cessation, revocation or activation of its certificates.

3) To immediately inform the relevant CGS and the subscriber (in the event that they are unaware) of any event (e.g. suspicion of exposure of private keys or verified request) requiring the cessation or revocation of a certificate in accordance with this Practice Statement.

4) To meet the applications for revocation, cessation or activation of certificates **immediately after** receipt and verification of the relevant application, according to the specific terms of this Practice Statement and Policy of the relevant certificate. In an emergency the procedure is carried out by calling the emergency certificate revocation line at +30 6951007878.

2.1.2 OBLIGATIONS OF LOCAL RA ASSISTANTS

The Local RA Assistants, acting as independent bodies that undertake the specific role and participating in the ATHEX network, accept the following obligations:

1) To contribute in updating and registering their subscribers, providing them with information and the necessary printed material which is distributed by ATHEX'S "Digital Certification Services'.

2) To gather and cosign the completed 'Subscriber Application and Agreement' forms of their environment and to forward them (within a reasonable timeframe) to the collaborating '*Registration Service*' for approval, in accordance with the terms hereof.

3) To procure the *'Subscriber Device Provision Service'* (or to have designated the procurement method in their contracts) with any 'Secure Signature Creation Device' (e.g. smart cards) for the proposed subscribers.

4) To immediately inform the '*Revocation Management & Status Service*' about each (specified in these Practice Statement and the relevant Certificate Policy) case or application which has come to their attention that requires certification suspension, activation or revocation.

2.1.3 OBLIGATIONS OF THE SUBSCRIBERS

The subscribers (certificate holder) to the '*X.A. Digital Certificates Services',* either as the subjects of the certification *(for personal certificates)* or as holders of a certified object *(e.g. for 'Trust-Server*™*' certificates*), have the following obligations:

1) To be informed about and know how to use the signature creation data, the digital certificates and their devices and generally understand the operation of the public key infrastructures (PKI) before taking any relevant action or using the certificate.

2) To have read, understood and agreed with all terms and conditions contained in the present ATHEX Certificate Practice Statement and in the relevant Certificate Policy being used.

3) To provide accurate information in respect of the data requested for both the generation and the renewal or revocation of a certificate and to verify the correctness of the generated certificate before using the certificate or the respective signature-creation data.

4) To immediately inform the '*Revocation Management & Status Service*' or the relevant *Local RA Assistants* of any change in the information stated during the application for generation of the certificate and to immediately request the suspension or revocation of the certificate when there is suspicion or knowledge that the signature creation data has been accessed or has been otherwise exposed by a third party.

5) To exclusively use the customized secure signature creation device (e.g. smart card) that may have been given to them for the creation of a signature in a manner that is appropriate and consistent with the relevant instructions and to refrain from exporting their signature creation data to another device.

6) To protect their 'signature creation data' (private keys), their device and their 'activation code' (PIN) from loss, disclosure or exposure to third parties and generally from any unauthorized or their lawful use.

7) To prevent, under penalty of paying damages to ATHEX or any other injured third party, from acts of alteration, modification, illegal replication and/or malicious usage of the signature creation data, the certificate generated to them by the ATHEX services network and the information (directories, revocation lists, regulation texts and policies, etc) published by ATHEX in its repository, which constitute fraud and/or threaten the integrity and reliability of the ATHEX certification services.

2.1.4 OBLIGATIONS OF THE USER (DEPENDENT PARTY)

Before deciding whether or not to rely on the contents of the certificate in order to proceed with a transaction, action or omission, or to acquire justified conviction for the authenticity of the signatory and the undersigned document (in the broad sense), the user (dependent party) of an ATHEX certificate has the following obligations:

1) To verify the authenticity and any termination or revocation of the specific certificate by referring to the 'CA certificates' and the relevant 'Certificate Revocation Lists' (CRL) that are published in ATHEX'S '*Repository*'.

2) To check whether the intended use of a certificate is permitted or not by the relevant certificate Policy, according to which it was issued.

3) To be aware of the limits of liability, disclaimers and limitation of warranties declared by the issuer of the certificate and the archiving period of the evidence, as mentioned in the policy of the specific certificate and the 'User/Recipient Agreement' that is published by ATHEX, which must be accepted by the user before any use of the services.

ATTENTION! ATHEX and its authorized partners involved in the provision of the certification services shall not assume any liability towards any user of its certificates in the event that such user has failed to perform the above obligations and such failure has in any way caused damages to the user.

2.2 GUARANTEES, DISCLAIMERS & LIMITATION OF LIABILITY

2.2.1 GUARANTEES

As the certification services provider, ATHEX **guarantees the accuracy and validity of its certificates** (in line with the conditions set forth in this Certificate Practice Statement and in the Policy of the respective certificate) to any third party that reasonably relies on these.

Specifically, regardless of the structure of its services, ATHEX **guarantees**:

- at the time of initial activation of the certificate, the accuracy of all information contained in the certificate, and the existence of all data required for its issuance, pursuant to this Certificate Practice Statement and to the respective Certificate Policy.
- that the signatory, whose identity is attested in the certificate, shall upon activation of the certificate, have possession of the 'signature creation data (private key) corresponding to the above or to the signature verification data (public key).
- that both the signature creation data and signature verification (public and private key) that it provides to subscribers/certified parties, may be used in addition.
- that it makes every reasonable endeavor to publish the revocations of its certificates pursuant to the terms and the procedure laid down in this Certificate Practice Statement and the respective Policy of each certificate.

2.2.2 DISCLAIMERS

As regards the above, ATHEX **shall not be liable** to any injured third party **or for the above** , where there has been no fault on the part of ATHEX with regards to the malfunction or failure that caused the damage to the third party or where ATHEX has acted in compliance with the provisions of the Certificate Practice Statement and the Certification Policies or where the injured party themselves or such other party —outside the ATHEX services provision network— has caused the damage by violating the terms and conditions of the respective Certificate Practice Statement and the relevant Certification Policies or has caused the damage through an incorrect, inappropriate or illegal act.

Furthermore, ATHEX **shall not be liable** (consequently neither will the third parties collaborating with it in providing certification services) for any malfunctioning of its services in cases of **force majeure**, including but not limited to earthquakes, floods, fires, etc., including cases of black-out, network communication problems and in general all external obstacles that may prevent the smooth delivery of its services and are not due to its fault nor could they be foreseen or could their consequences be limited.

Unless otherwise provided for in this Certificate Practice Statement or in the respective Policy of the Certificate, ATHEX **shall not guarantee nor will it be liable for** the appropriateness, quality, lack of error or fitness for a particular purpose of all related services, products and documentation that it provides or

offers. The services and products offered to its subscribers and third parties are provided by ATHEX and its network on an **"as-is"** basis and responsibility about whether they are suitable for the desired purpose or whether the subscriber should or should not rely on these **shall lie exclusively** with the ATHEX subscriber or the third party (recipient) that decides to rely on them.

Lastly, ATHEX shall **not be liable** for any indirect or consequential damages, criminal or disciplinary action or punishment, foregone profits or any other indirect consequences incurred by any party on the occasion of the use of or reliance on a certain certificate.

2.2.3 EXONERATION OF LIABILITY FOR CERTAIN ACTIVITIES

ATHEX does not recommend nor provide guarantee for the use of the electronic signatures and certificates it issues in particularly risky activities or in activities that require very high security levels including air traffic control, management of critical information and infrastructures about the life and care of patients, nuclear system control, management of power plants and in general the operation of systems whose possible malfunction would lead to disproportionately large damages as compared to the usual activities for which use of the certificates issued hereunder is intended.

2.2.4 ATHEX'S MAXIMUM LIMITS OF LIABILITY

If, despite the above disclaimers and the limitations to the guarantees it offers, ATHEX becomes liable to any third party or subscriber for a genuine error or inaction, condition violation, malfunction or inaccuracy in the services it offers, the maximum limit of liability assumed by ATHEX and the entire network of its services for each certificate and throughout the entire period of certificate validity may not be cumulatively greater than such amount as is specified as **"CSP Maximum Liability Limit"** in the respective Policy of the "harmful" Certificate and is proportional to the Class of the certificate and the usage that can be made of the certificate for the given Class**.**

2.2.5 SECURITY POLICY

ATHEX reserves the right to insure or not its third party liability that is related to the issuance of certificates for an amount equal to (or greater than) ATHEX'S **"Maximum Liability Limit"** which corresponds to every type and class of issued certificate (and which refers to the relevant Certificate Policy').

2.3 DATA PUBLICATION POLICY

2.3.1 ATHEX'S REPOSITORY

ATHEX'S Repository is a freely accessible online location where ATHEX'S Dissemination Service collects and publishes (*through relevant 'links'*) **all critical information** relating to the provision of certification services in electronic format such as the certificates of the Root CA and the Operational CAs, the *Directory* of the certificates issued to subscribers, the list of the suspended and/or revoked certificates (*CRLs*), the Summary Statement of Services (PDS), the current and previous versions of the Certification Practice Statement and the supporting Certification Policies, the contracts used for the subscriber and the recipient and other useful information.

The web site that hosts ATHEX'S 'repository' is located at **http://www.athexgroup.gr/el/web/guest/digital-certificates-pki-regulations** and is freely accessible to any interested party.

2.3.2 PUBLICATION OF THE STRONG CERTIFICATES DIRECTORY

With the generation and activation of a certificate, a **complete copy of the issued certificate** is published in ATHEX'S repository and is available for downloading by any party, unless the subscriber-holder has expressly indicated their objection in the shared publication.

Publication of certificates is done either by the LDAP protocol or other readable electronic format chosen by ATHEX.

2.3.3 PUBLICATION OF "CERTIFICATE REVOCATION LISTS '(CRLs)

ATHEX publishes the periodically issued '**Certificate Revocation Lists**' ('CRLs') in its Repository which includes all temporarily (ceased) or permanently revoked certificates.

These lists are updated at regular intervals, whether they remain unchanged or there are modifications (e.g. certificate revocation). In any case, any temporary (cessation) or permanent revocation of a certificate is published-even with an extraordinary publication of a new list - immediately after the examination of the verified application or if there is sufficient reason for the revocation or termination of the certificate.

In an emergency, the procedure is carried out by calling the emergency certificate revocation line at +30 6972999420.

The publication of certificate revocation lists (CRL) is done with the 'LDAP' protocol in accordance with the provisions in Chapter 5.2 "Description of CRL'.

2.3.4 PUBLICATION OF CERTIFICATION PRACTICE STATEMENT & CERTIFICATE POLICY

All versions of ATHEX'S '*Certification Practice Statement*' and '*Certificate Policy*' (current and previous), and a *'Summary Statement of ATHEX'S Services'* (which includes a summary of the main terms of the ATHEX'S Practice Statement and Policies) is published in **electronic format** (*.pdf, .doc or .html files*) in the ATHEX *Repository*.

Electronic or **printed formats** of the current 'Certification Practice Statement' and supported Certificate Policies are also available from cooperating Local RA Assistants and the ATHEX headquarters (see *Contact Details in paragraph 1.2.5*). At the same time, along with every '**Application - Subscription Agreement**' for the acquisition of an ATHEX certificate, ATHEX'S **'Summary Statement of Services' (***PDS***)** is mandatorily distributed - in printed form and in the language (Greek or English) that the candidate subscriber desires.

Revisions or modifications of the CPS that have been approved by ATHEX'S 'Policy Management Committee', are published in the ATHEX repository **at least forty-five (45) days prior to their activation** and their entry into force.

2.3.5 SECURE DISTRIBUTION OF PUBLIC KEY

The web site that hosts ATHEX'S 'repository' is located at **http://www.athexgroup.gr/el/web/guest/digital-certificates-pki-regulations and contains the public key.**

2.4 SUBJECT NAMING POLICY

At this stage, ATHEX does not allow the 'aliases' to be recorded on the certificates that it issues, thus, **all the subjects' names on the certificates must correspond to confirmed and comprehensible names**. The latter refer to the name of the natural person or the legal representative of the legal entity.

Especially in the case of certificates issued to natural persons, except for the subject's name, ATHEX includes a 'specific area' in the certificates which is the subscriber's '**Personal Identification Code**'(PIN), which ensures the uniqueness of the person in the ATHEX environment, even in the case that two subscribers have the same name.

On the other hand, for reasons of international compatibility, all the names given in the ATHEX certificates are expressed in **Latin characters** with the transcription of Greek characters according to the standard [ELOT 743] **or in English as it appears in an official document (e.g. passport)** or translated **into English** -where applicable.

More information about the type and form of the names is provided in paragraph 5.1.3 (under chapter 'DESCRIPTION OF CERTIFICATES'), while details about the content of the fields concerning the names of certificates' subjects and their relevant significance is stated in the relevant Policy of each certificate issued.

2.5 PRIVACY POLICY

ATHEX collects, processes, publishes and archives its subscribers' personal data in the fulfillment of the present and relevant contracts and compliance with the provisions of the relevant regulatory framework. The personal data collected and further processed, as defined in the relevant legislation (Law no. 2472/97) concerns data that is necessary for the provision of certification services to subscribers and their trading with ATHEX. Personal data is collected exclusively by the subscribers themselves during the registration or subscription renewal process and are kept even after the expiration or revocation of their certificates (See Chapter 2.6 "Information Archiving Policy') to be used to provide **evidence** in any "dispute resolution procedures" relating to their certification and for as long as it is necessary for the fulfillment of these purposes, simultaneously taking into account the specific requirements of the regulatory framework for electronic signatures, such as data archiving obligations.

ATHEX'S collection of personal data complies with the terms of Law no. 2472/1997, as in force on the Protection of Individuals with regard to the Processing of Personal Data and the Law no. 3471/06 on the protection of personal data in the electronic communications sector. Such data is **not used for other purposes,** unless the subject has given its explicit (and written) consent as defined in Law no. 2472/97.

The subscriber, at its absolute discretion, which is expressed in the certification application (which may also be amended later by means of a new written declaration to ATHEX), may or may not allow the publication of a **copy** of his personal certificate (and of his personal data that is stated thereon) in the ATHEX **Directory** for ease of verification of his digital signature by others.

ATHEX informs its subscribers of the provisions of article 11 of Law no. 2472/97. In any case the subscriber is entitled to contact the "Registration Service" of ATHEX'S network (which in this case is the "Data Controller") to make use of his rights of access, as stipulated in Articles 12 of Law no. 2472/1997.

In the event of cessation, ATHEX reserves the right, and subscribers explicitly consent once they are informed, to transfer all its records to a third party of its choice with a view to transferring its relevant activities to such third party.

2.6 DATA ARCHIVING POLICY

Once a **"qualified certificate"** issued by ATHEX'S Digital Certificates Services expires or is revoked, the following shall be **archived for thirty (30) years**:

- The subscriber's certificate and *logs* of major transactions concerning the certificate (such as certificate cessation, revocation or activation, renewals, etc) shall be kept in electronic format.
- All of the subscriber's identification documents and the signed "Application-Subscription Agreement", as well as information on each application for cessation, revocation, or reinstatement, dispute resolution or complaint handling in respect of a certificate shall be kept in hardcopy and electronic format.

At the same time, and during the same period, information shall be kept for the "Certificate Revocation Lists" issued and signed by the Issuers of "qualified" certificates.

This archiving is mandatory for 'qualified certificates' in accordance with point i of Annex II of P.D. 150/2001 on electronic signatures and aims **at providing certification evidence in dispute resolution procedures**.

For **other certificates** ('non-qualified') ATHEX is obliged to archive such data **for a period of five (5) years** of their expiry or revocation, unless otherwise provided in the certificate's Policy.

After the above time period, no guarantee is given to the subscriber-certified party or to any third party that relied on an ATHEX certificate with regards to the possibility of resolving disputes *(see following Chapter).*

2.7 DISPUTE RESOLUTION POLICY

Through the Complaint Handling and Dispute Resolution Committee (CHDSC), ATHEX offers its subscribers and third parties that rely on its certificates **reliable** (both legally and technically) **information** and clarifications on the data of the relevant certificates and **tips** for interpreting and resolving potential disputes related to certification and use of its electronic certificates.

Should interested parties wish to use the mediation service of the CHDSC, they must submit their dispute to the Committee in writing, and the Committee must respond in writing **within 30 days at the latest** from the time it received the written request for mediation.

Where the dispute is turned against ATHEX or a third party member of ATHEX'S network in the provision of certification services (complaint), the Committee shall not be obligated to reply to the request of the interested party where the latter has initiated court or any other proceedings against them before the end of the aforementioned 30-day period.

2.8 CONTROL COMPLIANCE POLICY

2.8.1 VOLUNTARY ACCREDITATION AND VERIFICATION

ATHEX intends on submitting an application for '**voluntary accreditation**' by the National Telecommunications and Post Committee (NTPC) which by law is responsible for the voluntary accreditation of Certification Service Providers in Greece, within six months of the NTPC Voluntary Accreditation Regulation being published.

2.9 PRICING POLICY & MONETARY REFUND

The collaborating Local RA Assistants freely form their own Pricing Policy for the registration and issuance fees or renewal of certificates that are issued by the network the XA Digital Certification Service, and for the provision of any customized ‘secure signature creation devices' to their subscribers.

The certificate cessation and revocation services, the generated certificate directory services and the certificate status services through published 'Certificate Revocation Lists' (CRL) **are provided free of charge.**

Where an application by a candidate subscriber is not approved by the RS, the subscriber is entitled to a full cash refund by the Local RS Assistant, which it may have made the payment.

Furthermore, if ATHEX proceeds with the revocation of a subscriber’s certificate without the fault or request of the latter, then ATHEX is required **either** to make a partial refund of the amount paid by the subscriber **or** to issue a new certificate, depending on the time remaining up until the normal expiry of the certificate.

2.10 INTELLECTUAL PROPERTY AND OTHER RIGHTS

ATHEX retains all intellectual property and industrial rights on its databases, the contents of its electronic pages, the electronic certificates it issues, the trademarks and logos, and all the texts it publishes.

The publication, reproduction or otherwise exploitation of all or part of this Certification Practice Statement by third parties without written permission **is expressly prohibited**.

2.11 INTERPRETATION AND ENFORCEABILITY

2.11.1 INCORPORATION WITH REFERENCE TO OTHER DOCUMENTS

This Certification Practice Statement, through '**incorporation by reference**' both in the ATHEX contracts with third-affiliated certification bodies and the 'Subscriber Agreements' with certified-holders, and the 'recipient contracts' with users (dependant parties) of the certificate, governs ATHEX'S relations with every contracting party along with the other terms of the contract and the terms specified in the relevant certificate policy.

2.11.2 CONFLICT OF PROVIONS AND ENFORCEMENT ORDER

Where there is conflict in the interpretation of the provisions of the Certification Practice Statement's Greek text with the same provisions of the text in English or in another language, the Greek text shall prevail.

In case of inconsistency of the Certification Practice Statement with terms of other contractual documents, the enforcement order is as follows: a) this Certification Practice Statement text, b) the relevant Certificate Policy text, and, c) the text of the 'Subscription Agreement' and 'User/Recipient Agreement' text.

2.11.3 MAINTENANCE OF VALIDITY OF NON-VOID TERMS

Where a term or provision of this Certification Practice Statement is deemed invalid or unenforceable for any reason, the remaining provisions shall continue to be valid as-are, unless, in essence, the invalid term affects the content of the remaining terms, so they are interpreted in a way that makes them valid, enforceable and consistent with the purpose of the original text.

2.11.4 APPLICABLE LAW - COMPETENT COURTS

Greek law shall be the applicable law and it is agreed that disputes related to the provision of the digital certificates services described herein shall be subject to the exclusive jurisdiction of the Courts of Athens.

PART III: OPERATING TERMS

3.1 CERTIFICATE APPLICATION AND APPROVAL OF ISSUE

3.1.1 HOW TO AND WHO CAN APPLY FOR A CERTIFICATE

Application for the issue of certificates from ATHEX'S Digital Certification Services can be made by **natural persons or legal representatives of legal entities** (*for the issuance of 'personal certificates' and/or their own 'certificates devices'*) **or by legal entities** (*only for the issue of their own 'certificates devices'*) whose identity is known to a '*Local RA Assistant'* that collaborates with the ATHEX network.

For this purpose, candidate subscribers complete and sign the relevant *'Application-Subscription Agreement'* that is provided by the Local RA Assistants, and submit the relevant supporting documents that proves their identity, or their relationship with the subject of the requested certificate.

3.1.2 COOPERATION OF THE LOCAL RA ASSISTANTS IN THE CANDIDATE SUBSCRIBER'S APPLICATION

The contracted Local RA Assistants of the ATHEX network are obliged to cooperate in the submission of a certificate application by a candidate subscriber.

Thus, the responsible Local RA Assistant officer (*Administrator*) receives the subscriber's completed application, after quickly checking its 'completeness' (according to the Policy of the said certificate), **he/she co-signs the application** and forwards it (*in a sealed envelope along with the signed 'Subscription Agreement' and the supporting documents submitted by the subscriber*) to the collaborating '*Registration service*' (RS) **for approval**.

3.1.3 APPROVAL BY THE REGISTRATION SERVICE

Being responsible for the final inspection of the application**,** and after carrying out the 'identification and authentication' procedure of the certification subject, according to the next Chapter, the RS **approves or rejects** the application **or requests the completion of missing information** directly by the applicant, **within five (5) working days at most** from receipt of the application.

If the application is approved, the RS collaborates with the *'Subscriber Device Provision Service*' (SDPS) that creates the subscriber's certified keys *(provided, of course, this is required by the policy of the said certificates, such as with personal 'Smart Sign™'* certificates*)*, and forwards the relevant order with the necessary content *(subject name or description and relevant public key)* of the certificate that needs to be issued to the *'Certificate Generation Service'* (CGS).

3.2 IDENTITY VERIFICATION & SUBJECT AUTHENTICITY

3.2.1 AT INITIAL REGISTRATION

At initial registration for the issuance of a certificate, it is necessary for the certificate Applicant (or his legal representative) to make his physical presence to the appropriate ATHEX department, the RS in particular. The latter must **examine and verify** the identity and authenticity of the certificate's subject and the actual possession (*Proof of Possession - POP*) of the certified signature keys, in accordance with the provisions of the relevant certificate Policy.

For this reason, the following information is requested and thoroughly checked by the network's RS at initial registration:

- The **identity of subscribers-natural persons** based on certified copies of their official identification documents (identity card, passport) and a solemn declaration signed by the applicant -the authenticity of the signature of which shall be certified by a public authority - which will state that the subscriber-natural person is an adult and is not under judicial or legal prohibition or under judicial perception.

- The **legalization of the subscribers-legal entities** and their representatives, on the basis of appropriate legal documents (e.g. statutes, Official Gazette circulars, Board decision, etc.),
- The **subscriber's relationship with the subject** of the certificate, as in the case of the certification of the subscriber's device (e.g. server), which arises from relevant documents (e.g. copy of 'domain name' agreement for the subscriber's server by any 'official administrator' *(Hostmaster)* of these names),
- The **possession of certified keys** by the subscriber, which is provided either with the appropriate technical process if they are already in the possession of the candidate subscriber (e.g., by creating a 'PKCS #12' type application), or with the generation of new keys by the subscriber by the collaborating SDPS of the ATHEX network.

3.2.2 ON THE CERTIFICATE REVOCATION & ACTIVATION REQUEST

The revocation request may be performed via the specially-designed web application through which the management of the qualified certificate is carried out. In addition, the suspension or revocation of the certificate may be made by ATHEX if the applicant's identity is verified by one of the following modes:

- either with the applicant's physical presence and the presentation of an official identification document (e.g. ID card) before the 'Revocation Management & Status Service' (RMSS) or one of the network's Local RA Assistants,
- or with the manually signed handwritten application by the applicant to the RMSS network,
- or (*only for the certificate's 'temporary revocation' (cessation)*) with the simple comparison of the personal data declared by the applicant/subscriber and the related data held on file by the RS network.

(According to this recommendation, the data that is requested and checked during a registration application should also apply in this case.)

3.2.3 ON THE RENEWAL OF A CERTIFICATE

3.2.3.1 Normal renewal

During the 'normal' certificate renewal process (i.e. before the set expiry of the current certificate) the holder may renew the qualified certificate via the specially-designed web management application.

Furthermore, the 'normal renewal' of a certificate is possible (i.e. before the set expiry of the current certificate) via the submission of an electronically signed 'renewal application' by the subscriber - based on the current certificate - where the subscriber **shall declare** that no modification has been made to the data of the preceding certificate or the relevant changes will be highlighted.

3.2.3.2 Renewal after expiration or revocation of the certificate due to key exposure

Regarding the renewal of certificates after their expiration or revocation due to exposure of the related cryptographic keys to risk (e.g. certificate theft), the holder may use the specially-designed web certificate management application to create a new certificate after removing the previously revoked or expired certificate. Moreover, a **new 'handwritten' application** may be used by the subscriber certifying the authenticity of his/her signature, however, without the resubmission of identification documents being required if the existing 'Personal Identification Number' in the ATHEX network (*see Chapter 2.4 "Subject Naming Policy'*) is stated in the application and invokes the same valid identification documents with those that had been provided during the initial registration. In the event that such a certificate is used by a legal representative of a legal entity, appropriate legalization documents must be provided (e.g. statutes, Official Gazette circulars, Board decision, etc.) that will prove the relationship between the applicant and the legal entity.

3.2.3.3 Renewal after revocation of the certificate (due to key exposure)

During the certificate renewal procedure after revocation caused for another reason other that the exposure of the subscriber's cryptographic keys (*e.g. in case of ATHEX'S revocation of the certificate due to the subscriber's failure to fulfill his financial obligations in time*) it is possible to circumvent the verification process of the subscriber's identity that is provided during the initial registration and for the RS to instruct

the CGS to issue of the new certificates, based on the existing data of the initial registration, provided the subscriber indicates their validity.

(According to this recommendation, the data that is requested and checked during a registration application should also apply in this case. Therefore the shaded parts of the application must be received.)

3.3 GENERATION OF KEY PAIR AND 'SSCD' DEVICE

3.3.1 SPECIFICALLY FOR PERSONAL CERTIFICATES

3.3.1.1 Creation and storage of keys in 'sscd' device

As soon as the RS **checks** and **approves** the applicant's application and the necessary documents that have been forwarded by the Local RA Assistants, it requests that the SDPS **creates an appropriate pair of encryption keys** (whose public key will be included in the certificate) and **safe storage** in the subscriber's customized 'secure signature creation device' (e.g. smart card), which is provided for this purpose by the Local RA Assistant cooperating in the application. In addition, the Subscriber is able to use the specially-designed web application to generate the requested Certificates. Consequently, the production of this certificate and asymmetrical cryptographic keys is fully transferred to the Subscriber.

3.3.1.2 Customization of SDPS device and registration of 'activation code' (PIN)

The device is **customized** by the SDPS in that the subscriber's name and the unique 'Personal Identification Number' (PIN) appears on the outside, and distinguishes the specific subscriber within the ATHEX network environment.

At the same time, the SDPS prints the device's 'activation code' (PIN) in a special opaque envelope and awaits the issuance and receipt of specific certificates from the CGS in order for these to be stored in the subscriber's customized device.

The above procedure, in combination with the secure dispatch of the device and the 'activation code' to the certified party, **ensures** the subscriber's exclusive possession of the specific private key (*'Proof of Possession'–'POP'*) that corresponds to the public key that is stated in the certificate.

Further to the creation of the Certificate by the subscriber via the specially-designed web application, the 'activation code' (PIN) is automatically generated and sent to the subscriber via the same application.

3.3.1.3 Delivery of the device to the subscriber

The delivery of customized device which contains the private keys and corresponding certificates, as well as the file with the activation code (PIN) of the subscriber's device is done with separate registered deliveries to the address that the subscriber has stated in his application.

The 'PIN' envelope can be sent to the subscriber directly from the SDPS, whereas the device can alternatively be delivered to the subscriber via the local RA Assistant.

Further to the creation of the Certificate by the subscriber through the specially-designed web application, the delivery of the device is carried out by the Registration Service during the initial registration provided that the application has been approved. If the subscriber desires, the device can be sent by registered mail to the address stated in his application.

3.3.2 SPECIAL CERTIFICATE DEVICES

3.3.2.1 Creation of Key Pairs

The creation of cryptographic key pairs for the subscriber's certified devices, is carried out within the device itself, using appropriate software that is able to create the **type** and **size** of the cryptographic keys that are required by the specific Policy of the certificate in question.

3.3.2.2 Proof of possession of the 'signature creation data' (private key)

Proof of possession of the specific private key ('*Proof of Possession'-'POP'*) by the subscriber-holder of their certified device, is done with the dispatch of a type 'PKCS # 12' online application to the Registration Service which includes and encrypted (with specific private key) section, which must be able to be decrypted by the RS by using the corresponding public key for which certification is requested.

3.3.2.3 Certificate delivery and installation

Delivery of the device's issued certificate is done via the "Dissemination Service" (DS), either via e-mail or by mailing a floppy disc that contains the certificate, to the address specified by the subscriber.

Upon receipt of the certificate, the subscriber must **install** it in the relevant device, by using the 'secret installation code' that was determined during the creation of certified keys.

3.4 CERTIFICATE GENERATION AND INITIAL ACTIVATION

3.4.1 GENERATION BY THE APPROPRIATE OPERATING CERTIFICATE AUTHORITY

When an electronically signed mandate for the generation of a certificate arrives from the RS to the 'Certificate Generation Service' (CGS), the latter mandatorily proceeds with the **generation of the certificate.**

The appropriate '*Subordinate or Operational CA'* service generates and signs the certificate, which should be authorized to issue these kinds of certificates that correspond to a specified "Certificate Policy" ('*CP*').

3.4.2 PROCEDURE FOR INITIAL CERTIFICATE ACTIVATION

For security reasons, every certificate that is generated by the ATHEX network, is placed in '**suspended**' mode (temporary revocation or 'cessation'-*see next chapter 3.7*) immediately after its generation until it is activated at the subscriber's request, following its receipt.

The initial activation procedure is described to the subscriber with the dispatch of **corresponding guidelines** for the activation along with the dispatch of the certificate's device.

The subscriber's initial activation application comprises of an online, postal or by fax dispatch of the subscriber's statement, which contains the following:

- the subscriber's acceptance of the correctness of the information contained in the received certificate,
- assurance that at that moment, the subscriber is the holder of both the private key device that was set during the generation of the certificate, and the relevant activation code.
- assurance that the subscriber is aware of the terms and conditions of use of the certificate that are included in the present Certification Practice Statement (*CPS*) and specific Certificate Policy (*CP*),
- finally, the subscriber's willingness for the certificate to be activated.

  As soon as the above statement is received by the subscriber, the '*Revocation Management & Status Service*'(RMSS) takes action to reinstate the validity of the certificates (initial activation), in accordance with the provisions of paragraph 3.7.3 SUSPENSION, REVOCATION AND (RE-) ACTIVATION PROCEDURE .

Moreover, where a Qualified Certificate is created by the subscriber, the certificate is activated directly from the specially-designed web application.

3.5 CERTIFICATE DURATION AND EXPIRY

3.5.1 CERTIFICATE VALIDITY

The validity of the certificates of end entities (*natural persons or objects-devices*) is specified in the text of the relevant Policy and is usually **one year**.

For the sake of better and bundled management of the renewal process (*see the next Chapter*) **the exact expiry date** of certificates issued to end entities by the ATHEX network, is calculated as follows:

- For certificates that are issued between the 1st and 15th day of the month, the first (1st) day of the month following the issue of the next or second following year is set as the expiry date (*depending on whether provided it is a yearly or biennial duration*)
- For certificates that are issued between the 16th and 31st day of the month, the fifteenth (15th) day of the month following the issue of the next or second following year is set as the expiry date (*depending on whether provided it is a yearly or biennial duration*)

(*Note: For the validity of the certificates (and cryptographic keys) of ATHEX'S 'Root Certification Authority "(Root CA) and the other "Subordinate CAs' (Operating CAs), see paragraph 4.1.1.3 in Chapter 'Technical Security Measures').*

3.5.2 AUTOMATIC EXPIRY OF CERTIFICATE VALIDITY

Upon reaching the validity expiry date, which is stated in a respective field within the certificates (*see Chapter 5.1 'DESCRIPTION OF* CERTIFICATES*'on certificate fields*), these **automatically lose their validity, without any other process being required**, such as e.g. the registration of the certificate in the 'Certificate Revocation List' (CRL).

The software and applications used by the subscriber or the certificate user (recipient) for the creation and verification of signatures, must be able to edit the related field on the expiry of the certificate and inform the user.

ATTENTION! Upon expiry of its validity, a certificate must not be used for any use, other than the verification or validation of electronic signatures that were created while relying on this certificate during its validity.

3.6 CERTIFICATE RENEWAL

3.6.1 RENEWAL SITUATIONS

The renewal of ATHEX'S certificates can be either **'ordinary'**, where the subscriber completes and electronically signs the renewal application that is sent by the network's RS before the expiry or revocation of his existing certificates, or '**extraordinary'**, where the subscriber's certificates have expired or have been revoked thus the subscriber is obliged to repeat the handwritten application and identification verification procedure as in the initial registration, according to the provisions of paragraph 3.2.3.2.

At the same time, when the Certificate is created by the subscriber, the Certificate renewal will be made directly from the specially-designed web application.

3.6.2 CONDITIONS FOR RENEWAL

Provided it has the Local RA Assistant's consent, the RS sends the subscriber an online renewal form to the e-mail that has been stated **twenty (20) days prior to expiration of the certificates**. If the certificate of the latter has been issued by ATHEX and the corresponding service, the subscriber needs to complete it, sign it electronically with the current certificate, and send it back to the e-mail address specified by ATHEX'S RS. Alternatively, if the certificate has been issued by the subscriber through the specially-designed web application, the online application does not need to be completed and sent. The certificate renewal will be carried out via this application.

If the certificate has been generated by ATHEX and the subscriber has not made use of the specially-designed web application, the online renewal form, and handwritten applications in case of an 'extraordinary' renewal, include data related to:

- Acceptance of the charge for renewal by the subscriber and the payment method,
- The agreement for the provision of the subscriber's new 'SSCD', which may be necessary for the renewal of personal certificates,

- The subscriber's statement that the documents that were submitted during initial registration remain valid, and that no changes have been made to the data of the subject that are included in the expiring certificate, or any of its modifications,
- Other possible declarations or notifications by the subscriber that may possibly be required by the particular policy of the Certificate being renewed.

3.6.3 CERTIFICATE RENEWAL METHOD

Certificate renewal entails the generation of new certificates for the subscriber with the same or appropriately modified data. Depending on the Policy provisions of the renewed Certificate, the creation of a new pair of encryption keys may be required for the new certificate. Especially for personal certificates, it is likely for the policy to anticipate the use of a new private keys and certificates device.

Moreover, the certificates are renewed by following the relevant procedures set out in this Certification Practice Statement and the generation of certificates following the approval of the initial registration, or through the specially-designed web application.

3.7 CERTIFICATE SUSPENSION AND REVOCATION

3.7.1 DEFINITION OF CERTIFICATE 'CESSATION/SUSPENSION' AND 'REVOCATION'

The **'cessation'** of a certificate involves -on one of the reasons mentioned in the next paragraph - the suspension of a certificate's validity**,** (which, however, may be reinstated with the certificate '(re-)activation' process, if it is confirmed that the above reasons have been eliminated), while the (final) '**revocation'** of the certificate entails definitive invalidity, without reinstatement being possible in any way.

3.7.2 REASONS FOR CERTIFICATE SUSPENSION AND/OR 'REVOCATION'

The reasons for suspension and (final) revocation **are common,** with the difference that the application and implementation of the suspension are imposed even at the slightest suspicion that one of the common reasons exists, whereas the application and realization of the revocation requires basic certainty that specific reasons exist.

Especially for the suspension of certificates, **the generation of certificates** is exceptionally provided as a reason under the definition of being on hold for the "initial activation" of the certificate by the subscriber after his receipt and/or installment.

Thus, according to the liable or the beneficiary of the suspension or revocation of a certificate that has been generated by the ATHEX network, the following reasons can be stated:

3.7.2.1 Reasons for revocation by the Services of the ATHEX Network

ATHEX'S network services are entitled to request the suspension or revocation of a subscriber's certificate, if:

- There are outstanding financial obligations regarding the generation of the certificate by the subscriber,
- It is imposed to maintain system reliability and Public Key Infrastructure (PKI) of ATHEX'S network, particularly where loss of control or lawful possession of the private key or the activation code is made known by the subscriber or if the network's RS has indications or proof of the non-correctness of the certificate data.
- This is imposed by a final court decision or another authority or court order (SECTION 1.3)
- It is imposed due to loss of the subscriber's legal capacity. (SECTION 1.2)

3.7.2.2 Reasons for which a Subscriber can submit a revocation request

The subscriber is obligated to request the suspension or revocation of a certificate when:

- He has lost control or lawful possession of the private keys or their activation codes,

- There is suspicion or certainty that the private keys or the activation codes have been exposed to third parties,
- Amendments have been made to any of his data that is stated on the certificate,
- He has lost his legal capacity (SECTION 1.2)
- He is obliged to act in accordance with the provisions of other sections of this Certification Practice Statement, the text of the Policy of the respective certificate or the Subscription Agreement.

Furthermore, the subscriber has the right to request the suspension or revocation of the certificate whenever he desires and without the application being required as justification.

3.7.2.3 Other reasons for Suspension or Revocation

Other reasons that may justify the suspension or revocation of a certificate are:

- The relevant provision (right or obligation) exists in other sections of this Certification Practice Statement, the text of the Policy of the respective certificate or the Subscription Agreement.
- At the request of a third party, on whose assurances the approval for the generation of the subscriber's certificate were based.

3.7.3 SUSPENSION, REVOCATION AND (RE-) ACTIVATION PROCEDURE

Both the suspension and revocation of a certificate are carried out by the RMSS that received the request with the entry of the unique 'Serial Number' that characterizes this certificate and the relevant revocation reason (see Chapter 5.2 'DESCRIPTION OF ‘CERTIFICATE REVOCATION LIST (CRL)' in particular) in a signed *Certificate Revocation List'-'CRL'* which is signed by the issuer of the certificate and is publicly published online.

The entry of a certificate’s 'Serial Number' in the CRL and therefore its suspension or (final) revocation, can be detected **either** by using special certificate validity verification software, **or** directly by the user who reads the list and compares the 'serial numbers' with the corresponding certificate of interest.

The network’s relevant RMSS is obligated to execute the suspension or revocation request that it receives **at most within 24 hours** of verifying the authenticity of the request (according to the provisions of the previous paragraph 3.2.2) and to inform the subscriber accordingly.

The validity of a suspended certificate is (re-)activated following the verified request by the party requesting the suspension with the issuance of a new CRL from the RMSS, at which time the entry in question is deleted.

If the Certificates have been issued by the subscriber himself, the latter is able to suspend, revoke and (re-)activate the certificate via the specially-designed web application. In case of a certificate suspension or revocation, the CRL is updated automatically by the specially-designed web application.

3.7.4 MANDATORY CERTIFICATE (RE-) ACTIVATION

Other than the certificates that have been (suspended) due to being in an issue and on hold status regarding the "initial activation" by the subscriber and whose validity is reinstated immediately after the receipt of the application of paragraph 3.4.2, the remaining ceased certificates **cannot remain in a cessation/suspended status for more than one (1) week**.

The subscriber, who is immediately informed of the suspension of his certificates by the RMSS, must justifiably request the (re-)activation of the certificate within the above timeframe, otherwise it shall be permanently revoked without ATHEX and its network bearing any liability.

If the certificate has been suspended by the ATHEX network for one of the reasons stated in paragraph 3.7.2.1 and it does not proceed with the permanent revocation of the certificate within the same period then its validity is automatically reinstated (reactivated) without the subscriber’s collaboration.

3.7.5 ISSUE FREQUENCY OF THE CERTIFICATE REVOCATION LIST (CRL)

The relative "Certificate Revocation List '(CRL) of each Operating Certificate Authority of the ATHEX network must be updated and re-published **at most every twenty-four (24) hours,** providing the serial number of the issue (*see Chapter 5.2*) and the exact date and time of the next ordinary publication.

Where it is deemed necessary by the RMSS, an '**updated extraordinary version**' can be issued and published, i.e. a new update CRL can be issued prior to its scheduled issue.

3.8 CHANGE OF 'PKI' INFRASTRUCTURE KEYS AND CERTIFICATES

The used keys and certificates of ATHEX'S PKI infrastructure (both of the Sub-CAs and the basic certificate by the Root CAs) are also subject to change (renewal) for security reasons (*see paragraph 4.1.1.3*).

For the smooth change of the Certificate Authorities' certificates and the maintainance of the end entities' certificate authentication verification ability via a valid 'Trusted Path' certificate the ongoing coexistence of two different certificates and corresponding cryptographic keys shall be provided for each certificate authority of the ATHEX network (with the exception of the initial operating period), in accordance with the following procedures:

3.8.1 CHANGE OF 'SUBORDINATE CERTIFICATION AUTHORITIES' CERTIFICATES'

The cryptographic keys and certificates of a (Subordinate) Certificate Authority of the ATHEX network have a validity of ten (10) years (*see paragraph 4.1.1.3*) and are used exclusively for the signing of end entity certificates (*that have a maximum duration of two (2) years*) and for signing the "Certificate Revocation List" CRLs for these certificates.

Two (2) years prior to the expiry of the certificates issued by the Sub-CAs (*i.e. the maximum duration of the certificates that they issue to end entities*), a **new pair of encryption keys** is created and a **new certificate** is issued for these CAs (by ATHEX'S Root CA), which is used **exclusively** -from that moment onwards- for signing **new** certificates that are issued for end entities and respective 'Certificate Revocation Lists' (CRL), while the previous certificate of the Sub-CA that remains in force, is used **only** -in the remaining term until its expiry- for signing CRLs that are stated in the certificates of end entities which had been issued under this certificate and which, are likely to still be in force.

3.8.2 CHANGE OF CERTIFICATE ISSUED BY ATHEX'S ROOT CA

Similarly, the cryptographic keys and self-signed certificate by ATHEX'S Root Certification Authority (X.A. Root CA) are valid for twenty (20) years (*see paragraph 4.1.1.3*) and are exclusively used to sign certificates by Sub CAs and for signing a "Certificate Revocation List" CRL that may arise for these certificates.

Therefore, **ten (10) years** prior to the expiry of the certificates issued by the Root CA (*i.e. the maximum duration of the certificates that they issue for the Sub CAs*), a **new self-signed certificate is issued at the same time** by the Root CA, which is used **exclusively** -from that moment onwards- for signing **new** certificates and the respective 'Certificate Revocation Lists' (CRLs) that are issued by the Root CA for its Sub CAs, while the previous certificate by the Root CA that remains in force, is used **only** -in the remaining term until its expiry- for signing one - not possible under normal circumstances - CRL that shall be stated in the certificates of Sub CAs which had been issued under this certificate and which are still in force.

3.9 CESSATION OF CERTIFICATION SERVICE BY ATHEX

If a decision is taken for ATHEX to cease the provision of digital certification services, the company undertakes the following actions:

- Timely notification -at least three (3) months prior- concerning the upcoming cessation of the services by any means to all parties that will be affected by this cessation (subscribers, recipients and customers).

- Revocation of all certificates issued by the ATHEX network and the cross-certification certificates that may have been issued to and from other certification bodies.
- Destruction of all private keys of the Root CA and the Sub CAs of the ATHEX network.
- Transfer of all the files and records stated in Chapter 2.6 ‘Data Archiving Policy' to an assignee body that will undertake to maintain the data for the period provided by the policies of the relevant certificates and by law.

To cover the cost of these actions, in the event that the cessation of ATHEX’S services is caused due to bankruptcy, the company will take out insurance coverage from a reliable insurance company.

PART IV: RELIABLE AND SECURE SYSTEM

4.1 TECHNICAL SECURITY MEASURES

4.1.1 CREATION OF CRYPTOGRAPHIC KEYS

All pairs of cryptographic keys that are generated for the Certificate Authorities (CAs), the Infrastructure's internal operations (PKI), and ATHEX'S Subscribers, are created using only ATHEX-approved hardware and software. Specifically, the creation of CA Certificate keys and certificates and PKI certificates are only carried out with the use of an approved and accredited card.

4.1.1.1 Creation and storage of keys by ATHEX'S Certification Authorities

The initial creation and storage of keys by ATHEX'S 'Root CAs' and 'Sub CAs' falls under a special '*Root Key Generation Ceremony for Certification Authority' w*ith the presence of independent third-party auditing bodies confirming compliance of all of ATHEX'S procedures and related security measures. All actions that are conducted during the ceremony are recorded and retained for any future auditing of the procedures.

The creation and storage of cryptographic keys by ATHEX'S 'Root Certification Authority' (*Root CA*) and every 'Subordinate Certification Authority' (Sub CA) is only prepared through a special **'hardware security module'** whose operation is certified by the standard [FIPS 140-2 level 3]. The use of "secure hardware unit" for the creation and storage of the cryptographic key pair for every ATHEX Certification Authority requires the involvement of at least two (2) different individuals acting in accredited 'trusted roles' *(see Chapter 4.3)***.**

4.1.1.2 Creating subscribers' keys (end entities)

ATHEX'S subscriber cryptographic keys are created, according to the provisions of the certificate policy, as follows:

- **either** by the 'Subscriber Device Provision Service' (for personal certificates of natural persons), which uses the '*Hardware Cryptographic Module*' for this purpose in accordance with the standard [FIPS 140-2 level 3], **or** by the Subscriber himself through the specially-designed web application.
- **or** by the Subscriber himself (mainly device certificates e.g. Servers), which must then use a *Software-based Cryptographic Module*, which complies with the above standard.

If the certified keys are created by the Subscriber himself, ATHEX does not provide any guarantee regarding the creation of the keys and is merely limited to indicating the appropriate software that is based on internationally-accepted industry standards. The ultimate responsibility for the correctness of the subscriber's key generation process, for which a certification application is sent to ATHEX, is undertaken by the subscriber himself.

4.1.1.3 Size and validity duration of the keys

The number of used keys is exponentially proportional to the security offered by their putative future 'decryption', but also proportional to the processing power that they require during their use.

On the other hand, the cryptographic keys used in ATHEX'S PKI infrastructure have a limited validity duration and are subject to regular expiry, revocation and renewal (as are their corresponding certificates) for security reasons.

Thus,

- the cryptographic keys by ATHEX'S '*Root CA'* have a key size of **2048 bits** and a duration of **20 years** (as do their corresponding certificates).
- the cryptographic keys by ATHEX'S '*Subordinate CAs'* have a key size of **1024 bits** and a duration of **10 years** (as do their corresponding certificates).

- the cryptographic keys by ATHEX'S *Subscribers* have a key size of at least **1024 bits** and a duration of **1** (as do their corresponding certificates), depending on the provisions of the relevant Certificate Policy.

Note: See paragraphs 3.8.1 & 3.8.2 for the key change and certificates procedure of ATHEX'S Root CA and Operating Certificate Authority and paragraph 3.6 as well as the relevant paragraphs of the corresponding Certificate Policies for the key renewal and certificates procedures of end entities (subscribers).

4.1.1.4 Algorithms used by ATHEX

The algorithm used to create the encryption keys for all of ATHEX'S Certificate Authorities (and for subscribers' keys, that are created by the SDPS) is the algorithm [Rivest - Shimar - Adleman Algorithm] **(RSA)**'.

The algorithm used for Hashing when creating an advanced electronic signature is the [Secure Hashing Algorithm - 1] **(SHA-1)**.

4.1.2 PROTECTION OF PRIVATE KEYS

4.1.2.1 Secure creation procedure and compulsory use of private key device

All cryptographic key pairs that are certified by ATHEX'S Digital Certification Services must be generated as such that the Private key cannot be known to anyone else other than the holder of those keys.

To achieve this, the private keys generated by ATHEX are stored in secure devices (e.g. separate cryptographic modules or smart cards) which require the use of a special '**activation code**' *(see below)*, which is known only by the authorized user. These devices must be sent to the eligible subscribers and this is done by registered mail which requires a signature as evidence of receipt.

By exception, if it is expressly permitted by the relevant certificate policy that is issued to a subscriber, the relevant private key can be stored on a floppy disk and/or 'non-shared hard disk' held by the subscriber.

Furthermore, private keys of the certificates can be produced directly into the device that the subscriber possesses through the specially-designed web application. This method ensures that the private key will not be disclosed to third parties other than the holder.

4.1.2.2 Back up, storage and retrieval of private keys

The creation, storage, use, back up and retrieval of cryptographic keys by ATHEX'S Certification Authorities is always done by using a special '***Hardware Security Module'*** whose operation is certified by Standard [FIPS 140-1 level 3], while *every act* requires the involvement of at least two (2) different individuals that have accredited 'trusted roles' *(see Chapter 4.3).*

Encrypted *backups* of private keys by ATHEX'S Certification Authorities (*CAs*) are held-for their potential use e.g. destruction of original key device - in 'safe areas' within and outside of ATHEX'S premises *(see paragraph 4.2.1)*.

No private key that is generated for a subscriber by the 'Subscriber Device Provision Service' and no private key of the CSP, is backed up or stored in any way (e.g. with the sharing method or else '*Key Escrow*') that could contribute in their recovery by ATHEX'S Services or anyone else.

If the keys have been created by the subscriber himself (provided this is permitted by ATHEX'S relevant certificate policy), the subscriber assumes full responsibility as to the whether copies of private keys will be copies or not and their mode of protection.

4.1.2.3 Private key device activation code

All the private keys used in ATHEX'S Digital Certification Services (Generation Authorities, internal operation of the PKI and Subscribers) regardless of the storage medium, must **mandatorily** be

protected with secret '**activation code**' (*PIN*) which allows the activation and use of the private keys or the device containing the private keys, only by the authorized person that knows it.

The subscribers' private key device **activation codes** which are generated by the 'Subscriber Device Provision Service', comprises of an alphanumeric code made up of 8 digits, which is printed in a protected folder that is immediately sent to the respective subscriber **without being registered or memorized in any way by this or any other ATHEX Service**.

Further to the creation of the Qualified Certificate by the subscriber via the specially-designed web application, the 'activation code' (PIN) is automatically generated and sent to the subscriber via the application.

(ATTENTION! Improper retention of the delivered device's activation code by the subscriber in conjunction with the loss of the printed copy contained in the above envelope, results in the **permanent failure to active the private keys** contained in this device!).

4.1.2.4 Limited use of private keys

The cryptographic keys that are certified a part of ATHEX'S PKI infrastructure have **limited uses** that are defined according to their relevant Certificate Policy.

Specifically, the private keys of all of ATHEX'S Certification Authorities ('Root CA' and 'Operational CAs') are certified to be used **exclusively** for signing 'Certificates' (either by CAs or "end entities") and relevant 'Certificate Revocation Lists' ('CRL'). **These certificates cannot be used for any other reason**.

Similarly, the private keys of end entities are certified for use in other specific uses (e.g. for signing documents, signing emails, authentication, data encryption, etc) **depending on the specific 'Certificate Policy' (CP) under which they are issued**.

4.1.2.5 Destruction of the Certification Authorities' private keys after their expiry

Both the original and the reserve (back-up) private keys by ATHEX'S Certificate Authorities are destroyed after the expiry of their validity in order to guarantee their non-recovery and reuse.

This destruction is either effected by destroying the private key device in the event that it is a smart card or magnetic device e.g. CD-ROM), or by disabling and reconfiguring the cryptographic module in which they are held.

The destruction process of withdrawn private keys issued by ATHEX'S Certification Authorities is supervised and recorded and relevant records are archived.

4.1.3 OTHER TECHNICAL SECURITY MEASURES

ATHEX takes all possible and appropriate means and techniques to protect and reassure the system against internal or external threats, such as the attack of central servers from malware, hacking, entry errors, etc.

Indicatively, ATHEX takes the following measures:

- Network protection using '*firewalls*',
- The use of special '*Hardware Security Modules*' whose operation is certified based on standard [FIPS 140-2 level 3],
- The issue and use of personal keys and certificates for the operation of the PKI systems for each authorized user in the system (see the following paragraphs as well)
- Network design with the shortest possible routes between the necessary *servers*,
- Strict limitation of terminals with access to the system of the absolutely necessary and with the exclusive use of authorized users,
- Check for viruses in any software that needs to be installed on the system, etc.

4.2 PHYSICAL SECURITY MEASURES

The physical security measures concern all the areas in which key functions of ATHEX'S PKI infrastructure are performed, specifically including the functions of the 'Root Certification Authority', the 'Subordinate Certification Authorities', the 'Registration Services' and 'Subscriber Device Provision Service'. If some of these services have been outsourced to ATHEX'S partners, they too are subject to the same physical security measures in the areas where these services are performed.

4.2.1 SELECTION AND CONSTRUCTION OF AREAS

The functions of ATHEX'S PKI infrastructure and related equipment is installed in a building in order to limit unauthorized access. Personnel working with the data and equipment of the PKI infrastructure are located in areas that are isolated from others that are not intended for safe operations. The entry-exit points of these areas are limited to the minimum extent that is permitted by fire safety rules.

Areas in which the PKI infrastructure data is processed and/or stored and in which the relevant equipment is established, are designed as '**secure areas**', in which special considerations has been given to the planning of the air conditioning systems, power supply and telecommunications infrastructure.

A sign that states '*Authorized Personnel Only*' or a message to that effect is affixed to the entry of the above areas.

4.2.2 PHYSICAL ACCESS

Entry to the PKI infrastructure areas is protected with security doors bearing a locking mechanism. Every access to these areas is supervised and controlled by the control mechanisms that operate on an ongoing basis. The security areas are monitored even during non-working hours with sensor detection and alarm systems.

Unauthorized personnel and any visitors that must enter the secure areas must be accompanied by authorized personnel throughout the duration of their stay therein.

Access to all security areas requires the use of control techniques such as passwords, magnetic cards and/or a reception desk. All access rights in specific areas, security lockers and sensitive documents, and distributed access tools, such as keys, magnetic cards and tabs-badges are recorded in special 'access control lists'.

Every visit to the secure areas by visitors, external system maintenance and supply crews as well as authorized personnel outside of working hours is entered in an '*Access Control Log*'. These entries include the following details:

- *Identity and status (personnel or partner) of the incoming individual,*
- *Specific areas that may be visited,*
- *Exact time of entry and exit,*
- *Identity of entry supervisor.*

4.2.3 POWER SUPPLY, AIR CONDITIONING, FIRE SAFETY AND LEAKS.

The power supply to the central systems of ATHEX'S PKI infrastructure and Directories is protected against power failures. Special system backup and restoration procedures are in place to prevent data loss and to maintain high levels of availability.

The air conditioning in the security areas provides the appropriate temperature environment for the operation of equipment and personnel. Its installation is designed so as not to affect the area's physical security or the operation of the equipment in case of malfunction.

The security areas are protected by a fire detection and automatic fire extinguishing system. Finally, all measures have been taken to protect against plumbing leakages and generally the infrastructure system's exposure to water.

4.2.4 STORAGE OF DATA MEDIA

Data media and their copies, which are used to operate the system, are stored in secure cabinets that protect them from environmental threats such as temperature, humidity and magnetic fields.

4.2.5 AVAILABILITY OF TOOLS AND DATA SECURITY

The availability of access tools to physical areas and other security data such as activation codes and operation files, is done with secure and controlled procedures.

4.2.6 REMOTE ALTERNATIVE SYSTEM AND BACKUPS

A **second alternative system**, able to cope with all the certification services' key functions (certification management and publication of directories) is maintained by ATHEX in a remote location away from the original system.

4.3 CONTROL AND SECURITY OF PROCEDURES

The various internal security procedures that are followed in connection with the provision of certification services are described in more detail in ATHEX'S internal -unpublished- 'policy and security practices' texts.

4.3.1 TRUSTED ROLES

It is designated for the purposes of this text that all employees, contractual partners and consultants of ATHEX'S 'Digital Certification Services' that have access to or control cryptographic operations related to the generation, use, suspension or revocation of certificates, and the management of published directories, and the 'repository', serve '**trusted roles**'. Included in the personnel of 'trusted roles' are the system's administrators, technician and other operators as well as those persons that are assigned to supervise the operations of ATHEX'S 'PKI' infrastructure.

4.3.2 TRUSTED ROLES OF THE CERTIFICATE GENERATION SERVICE

The Certificate Generation Service (CGS) personnel has been allocated to 'trusted roles', each of whom undertakes predesigned procedures with limited and controlled access to the work required to be performed in order for the service's obligations to be completed.

4.3.3 TRUSTED ROLES OF THE REGISTRATION SERVICE & REVOCATION MANAGEMENT AND STATUS SERVICE

ATHEX takes all appropriate measures to ensure that the personnel of the certificates' Registration Service (RS) and the Revocation Management & Status Service (RMSS) comprehend their responsibility for verifying the identification and authentication of candidates or registered subscribers, while performing the verification functions and approval of an application for generation, revocation, suspension or reactivation of a certificate and for the safe transfer of data by the applicant to the Certificate Generation Service and the identification or subscriber activation codes.

ATHEX may allow the execution of all the operations of the Registration Service and the Revocation Management & Status Service to individual 'trusted roles' that will be assigned to trusted persons.

4.3.4 NUMBER OF PERSONS REQUIRED FOR THE EXECUTION OF A TASK

To ensure that the security regulations are not circumvented by a person acting alone, the administration and operations of ATHEX'S Digital Certification Services are distributed to multiple 'trusted roles' and corresponding individuals. Every access account to the ATHEX system will have limited capabilities taking into consideration the 'role' of the individual holding that account.

For this reason, every ATHEX Digital Certification Services personnel will be subject to verification of their identity and powers, **before**:

- *being included in the lists of individuals with access to secure areas,*
- *gaining an access account to the system and equipment,*
- *receiving the necessary certificate to perform their role.*

All the system Administrators' rights are controlled and certified with the issuance of special 'administrator certificates' which are required for access to the administrative operations of ATHEX'S Digital Certification Services.

Such a certificate (and related access account) has the following features:

- *it is directly associated with a specific natural person,*
- *use by anyone else is prohibited,*
- *its use is restricted to acts permitted by the specific roles of the holder, the operating system and the procedural controls with the use of special software.*

These administrator certificates are installed in special tokens (e.g. smart cards) that require an 'activation code', thus ensuring the utmost security of ATHEX'S Digital Certification Services operations.

4.4 PERSONNEL CONTROL AND RELIABILITY

4.4.1 REQUIRED EXPERIENCE, ACCREDITATION AND TRUST

ATHEX ensures that all the personnel that undertakes 'trusted roles' and responsibilities relating to the operation of Digital Certification Services:

- *have been positively evaluated in personnel security tests*
- *are bound by a contract or declaration for assumption of the specific role and the related terms and conditions,*
- *have received appropriate training for the assigned role and tasks,*
- *are bound by contract or declaration on the confidentiality and non-disclosure of sensitive information related to the security of ATHEX'S system and the subscribers' personal data,*
- *do not undertake any other duties that may come into conflict with their obligations and duties of ATHEX'S Digital Certification Services.*

All the above personnel implement and apply the company's management and personnel policies which determine the necessary levels of the personnel's reliability and competence for the satisfactory execution and performance of the Digital Certification services in a manner that is consistent with this Certification Practice Statement.

4.4.2 TRAINING REQUIREMENTS

ATHEX provides its personnel with special training regarding the execution of their duties and organizes additional seminars when training is needed for up-to-the-minute issues. Training includes:

- *The principles and the security mechanisms of ATHEX'S 'Digital Certification Services*',
- *All PKI software versions used by the ATHEX system,*
- *All tasks and procedures of the PKI system that must be observed,*
- *The company's Security Policy and Privacy Policy,*
- *The personnel's duties and obligations,*
- *Security violation and confidentiality reporting procedures.*

The above staff training is repeated periodically (e.g. annually or biennially) for maintaining awareness and knowledge on new policies and procedures.

Included in the personal file of every company trainee is a 'certificate of attendance' of the training program which is signed by ATHEX'S Digital Certification Services senior management.

4.4.3 CONTROLS AND PENALTIES

ATHEX conducts appropriate controls of all personnel to be used in 'trusted roles' (prior to these roles being delegated and thereafter on a periodical basis, if necessary) to confirm the reliability and adequacy of their qualifications in relation to the requirements of this Certification Practice Statement and ATHEX'S general personnel policy. Personnel that does not meet the relevant criteria during the initial or periodic controls shall not be used or will stop being used in 'trusted roles'.

If it is proven or there are strong indications that personnel that is responsible for tasks related to the operation of ATHEX'S Digital Certification Services conducts an act that is contrary to the regulations or their authority, their access to ATHEX'S system will be immediately suspended. Where it is proven that the same individual has conducted gross negligence or malicious intent, all privileges and access rights to the system will be permanently revoked and they will be subject to corrective and disciplinary procedures.

4.4.4 CONTRACTED PARTNERS' PERSONNEL

ATHEX ensures that its contracted partners involved in the provision of certification services and their relevant personnel will have access to the areas and ATHEX'S system only after authorization is granted or in the company of appropriate ATHEX personnel and every such event shall be entered in the relevant log book or electronically.

Every ATHEX contracted partner shall be subject to the term that they and their personnel are committed to complying with all ATHEX'S policies and procedures concerning the security and confidentiality of the system's data, concluding a 'Non-Disclosure and Privacy Agreement'.

4.4.5 PROVISION OF GUIDELINES AND DOCUMENTATION

All of ATHEX'S Digital Certification Services personnel is provided with comprehensive guidelines and any necessary documentation on procedures concerning the generation, update, renewal, suspension and revocation of certificates and the operation of the relevant software.

PART V: DESCRIPTION OF CERTIFICATES & CRLs

5.1 DESCRIPTION OF CERTIFICATES

5.1.1 VERSION TYPE AND NUMBER

ATHEX'S 'Digital Certification Services' use online certificate [X.509, Version 3] (3rd version), which support the use of *extensions*. The version number always refers to the relevant field of the certificate.

5.1.2 CONTENT AND SIGNIFICANCE OF THE CERTIFICATE FIELDS

Certificates that are issued by ATHEX to subscribers/end entities (*end-entities certificates*) have the following fields:

Field name (*)	Required	Content	Remarks
Version ***Version***	YES	"V3"	*Version '3' of online certificate 'X.509 - RFC 5280 CRL' supports extended fields*
Serial number ***Serial Number***	YES	[Integer]	*Unique number of the certificate generated by the specific Certificate Authority*
Signature Algorithm ***Signature Algorithm***	YES	[Identifier]	*Specifies the algorithm used for hashing and signing the certificate.*
Issuer ***Issuer***	YES	(Distinguished Name (DN) type 'X.501' for the Issuer)	*The name of the authority, analyzed into sub-fields. See analysis in the following paragraphs 5.1.3.1 and 5.1.3.2*
Valid from ***Valid From***	YES	[Date]	*The certificate issue date.*
Valid to ***Valid To***	YES	[Date]	*The certificate expiry date.*
Subject ***Subject***	YES	(Distinguished Name (DN) type 'X.501' for the subject)	*The name of the subject (holder of the certified public key), analyzed into sub-fields. The used sub-fields and their content is defined in the relevant certificate policy. See paragraph 5.1.3.3*
Public Key ***Public Key***	YES	[Hexadecimal number 1024]	*The certified 'Public Key' of the 'Subject'*
CRL Distribution Points ***CRL Distribution Points***	YES	(In the subfield '*Distribution Point Name:/Full Name:*=') [Address type 'URI']	*The address where the relevant updated "Certificate Revocation List" ('CRL') is published*
Certificate Policies ***Certificate Policies***	YES	[Policy Identifier] (& the subfield 'Qualifier: CPSUri: = ') [Address type 'URI']	*It contains the identification number (OID) that corresponds to the published text of a 'Policy' that governs the terms of use of the certificate and the electronic address in which this Certification Practice Statement is published*
Key Usage ***Key Usage***	YES	(Indications for usages authorized by the policies of the certified key)	*Defines the permitted uses of the subscriber's private key (e.g. identification, non-repudiation, data encryption, signature, etc)*
Extended Key Usage ***Extended Key Usage***	Optional	(Indications for extended usages of the certified key)	*Identifies extended usages of the subscriber's private key (e.g. signing code, secure e-mail, time stamping, etc)*

Authority Key Identifier ***Authority Key Identifier***	OPTIONAL	[Integer]	*Defines which Certificate Authority key pair was used to sign this certificate*
Subject Key Identifier ***Subject Key Identifier***	OPTIONAL *(in the certificates by* CAs*)*	[Integer]	*Defines which Certificate Authority key pair is certified with this certificate*

(*) = The field names appear in Greek or English depending on the language of the application used to 'read' the certificate (e.g. *MS Outlook Express*).

Also, the certificates issued by ATHEX can also have (optionally) additional fields that contain text-statements on the specific terms of use (e.g. maximum allowable transaction limit) of the certificate, and other fields with the certificate's attributes, e.g. its imprinting and the relative imprinting algorithm, etc.

5.1.3 FORM AND CONTENT OF DISTINGUISHED NAME (DN)

The distinguished names (*'DN '*) that are contained in the 'Authority' and the 'Subject' fields (certification subject) of the ATHEX certificates in the form of standard [X.501, Name] comprising of subfields with specific attributes. These attributes (such as Name, Surname, Country, etc) are defined in further detail in [X.520].

The contents of these subfields are written in Latin characters either in a faithful translation of their contents in English, or the transcription of Greek characters according to standard [ELOT 743] for international compatibility. *(see relevant paragraph 2.4 'Subject Naming Policy')*

5.1.3.1 Distinguished name (DN) of ATHEX'S 'Root Certification Authority'

The distinguished name (DN) of ATHEX'S 'Root Certification Authority', which is recorded in the 'Issuer' field in the '*CA Certificates'* -and in the '*Subject*' field in '*self-signed certificate*', has the following content:

Subfield	Explanation	Content
O =	Organization ***(Organization)***	**ATHENS STOCK EXCHANGE**
CN =	Common name ***(Common Name)***	**ATHEX Root CA G2**
C =	Country ***(Country)***	**GR**

5.1.3.2 Distinguished name (DN) of ATHEX'S 'Operating Certificate Authorities'

The distinguished name (DN) of ATHEX'S 'Operating Certificate Authorities', which is recorded in the 'Issuer' field of the 'Subscriber/end-entities certificates and in the 'Subject' field of the 'CA Certificates' that are issued by the 'Root CA' has the following content for each of the 'Operating Issuers' of ATHEX'S 'Certificate Generation Service:

A) ATHEX **General Certificates** CA **Class 1**:

Subfield	Explanation	Content
O =	Organization ***(Organization)***	**ATHENS STOCK EXCHANGE**
CN =	Common name ***(Common Name)***	**ATHEX General Certificates CA G2**
C =	Country (***Country)***	**GR**

B) ATHEX **Qualified Certificates** CA **Class 1**:

Subfield	Explanation	Content
O =	Organization ***(Organization)***	**ATHENS STOCK EXCHANGE**
CN =	Common name ***(Common Name)***	**ATHEX Qualified Certificates CA G2**
C =	Country (***Country)***	**GR**

5.1.3.3 Distinguished name (DN) of the 'Subjects' (Subjects-Subscribers)

The distinguished name (DN) of ATHEX'S 'Subscribers' that is recorded in the 'Subject' field of the 'Subscribers/End-entities Certificates issued by ATHEX, is defined - in terms of its structure - in the corresponding 'Certificate Policy', depending whether it relates to the subscriber's "personal certificates" or "certificates devices'.

5.1.4 CHARACTERIZATION OF EXTENSION CRITICALITY

Although all the certificate fields are considered 'critical' in the sense that they contain essential information for the Issuer, the Subject, the Certificate and the Terms of Use, certificate extensions [X.509 - RFC 5280] can be labeled as 'Critical' in the sense that an automated identification application cannot proceed with the acceptance of the certificate if it cannot interpret the content of such a field.

In the ATHEX certificates the '***Key Usage***' field is characterized as 'critical'.

5.2 DESCRIPTION OF 'CERTIFICATE REVOCATION LIST (CRL)

5.2.1 VERSION TYPE AND NUMBER

The CRLs that are issued by ATHEX'S 'Digital Certification Services' use the form that is consistent with the specifications [X.509, CRL Version 2] (2nd edition), which supports the use of extensions. The version number always refers to the relevant field of the certificate.

5.2.2 CONTENT AND SIGNIFICANCE OF CRL FIELDS

The CRLs that are issued by the RMSS and are signed by the 'Operating CA' of ATHEX'S network relating to subscribers/end entity certificates (and those issued by the Root CA for any revoked certificates of the network's CAs), have the following fields:

Field Name	Required	Content	Remarks
Version ***Version***	YES	"V2"	*Version '2' of standard 'X.509 - RFC 5280 CRL' supports extensions.*
CRL Serial Number ***CRLNumber***	YES	[Integer]	*Unique serial number that identifies the specific CRL.*
Signature Algorithm ***Signature Algorithm***	YES	[Identifier]	*Specifies the algorithm used for the hashing and signing of the list.*
Issuer ***Issuer***	YES	(Distinguished Name (DN) type 'X.501' for the Issuer)	*The name of the issuer (who signs the CRL) analyzed into sub-fields. See analysis in paragraph 5.1.3*
This Update ***This Update***	YES	[Date]	*The issue date and time of this CRL update.*
Next Update ***Next Update***	YES	[Date]	*The date and time of the next scheduled CRL issue.*
Authority Key Identifier ***Authority Key Identifier***	NO	[Integer]	*Identifies which of the Issuer's key pair corresponds to specific CRL (from which it was signed).*
Revoked Certificates ***Revoked Certificates***	YES	[Certificate List]	*The updated master list with information regarding revoked certificates up to the CRL issue. (See table below).*

Within the 'Revoked Certificates' field (which includes the main revoked certificates list) are the following sub-fields, which are repeated to describe each of the revoked certificates:

Field Name	Required	Content	Remarks
Revoked Certificate ***User Certificate***	YES	[Integer]	*The certificate's unique 'serial number' is revoked (-which was acquired from the particular Issuer)*
Revocation Date ***Revocation Date***	YES	[Date]	*The date and time of CRL issue with which this certificate was revoked.*
CRL Serial Number ***Reason Code***	YES	(Byte with indications on the ground that the revoked certificate - according to RFC 2459 or the relevant current standards)	*Identifies the reason for revoking the certificate e.g. revocation due to key exposure or simple cessation (temporary revocation)*
Invalidity Date ***Invalidity Date***	NO	[Date]	*The date and time of the certificate's revocation request.*

5.2.3 CHARACTERIZATION OF EXTENSION CRITICALITY

Although all the CRL fields are considered 'critical' in the sense that they contain essential information for the Issuer, the Revocation Date, the Certificate being revoked and the Reasons for revocation, the extensions of a CRL can be labeled as 'Critical' in the sense that an automated identification application should proceed with processing the CRL in question if it cannot interpret the content of such a field.

No field is labeled as 'critical' in the CRLs that are issued by ATHEX.