DIGITAL CERTIFICATION SERVICES

NON QUALIFIED CERTIFICATE POLICY

'SMART-SIGN™' (Double Key) - CLASS 1)

(Version 1.1 – 15/03/2016)

INCLUDES POLICIES FOR THE CERTIFICATES:

1. Authentication Personal Certificate SMART-SIGN™ Class 1
(*for Authentication at Applications*)
(1.

Policy Identifier (OID): ***1.3.6.1.4.1.29402.1.2.2.1.1.1***

2. Personal Certificate
(*for economic transactions*)
(2.

Policy Identifier (OID): ***1.3.6.1.4.1.29402.1.2.2.1.1.1***

3. Encryption Personal Certificate
(*for Data Encryption*)
(3.

Policy Identifier (OID): ***1.3.6.1.4.1.29402.1.2.2.1.1.1***

{ deliberately empty}

TABLE OF CONTENTS

POLICY FOR PERSONAL CERTIFICATES

SMART-SIGN™ (DOUBLE KEY) OF ATHEX

CLASS 1

IMPORTANT STATEMENTS:

1) The issuer of personal ***SMART-SIGN™ -Class 1*** certificates which comply with these policies **(**with **OID: 1.3.6.1.4.1.29402.1.2.1.1.1.1 and 1 1.3.6.1.4.1.29402.1.2.2.1.1.1) states** that he sets "**a limit to the value of transactions**" where such certificates can be used, except for the certificate for financial transactions, which is set to 14}EUR 0 (non-financial transactions), in accordance with Greek Presidential Decree 150/2001 on electronic signatures and its annexes (I and II) issued in compliance with Directive 99/93/EC on electronic signatures.

2) The issuer of personal ***SMART-SIGN™-Class 1*** certificates which comply with these policies (with **OID**: **1.3.6.1.4.1.11774.1.2.2.1.1.5 and 1.3.6.1.4.1.11774.1.2.1.1.1.5) guarantees** that the critical information material necessary for the use and support of the probative function of the certificate "**will be filed and be available** -on request with legitimate interest- **for 30 years**" after the expiry of the certificate, in accordance with Greek Presidential Decree 150/2001 on electronic signatures and its annexes (I and II) issued in compliance with Directive 99/93/EC on electronic signatures.

1 INTRODUCTION

1.1 GENERAL OVERVIEW

1.1.1 ATHEX personal SMART-SIGN™ (double key) certificates

The "*Digital Certification Services*" of ATHEX SA have created, support and manage —by way of the Policy Management Committee— electronic personal **SMART-SIGN™ (double key)** certificates to certify electronic signature verification data (public keys) for **natural persons**. The **SMART-SIGN™ (double key)** type is characterized by the parallel issuance and management **of two different supplementary certificates** (*which correspond to two different pairs of cryptographic keys)* **on a personalized device** which is a secure signature creation device.

Using this scheme, the *Digital Certification Services* of ATHEX SA (hereinafter ATHEX), allow the co-issuance and co-existence of:

(a) one **qualified personal certificate** (*for the secure signing of electronic documents which are equally valid as if they had been signed by hand*); and

(b) one **personal authentication certificate** (*for the secure identification and authentication of its holder by compatible telematics applications*),

through the **easy use of a common device** (and the use of common activation code, PIN), **while complying with the strictest specifications** in line with Greek Presidential Decree 150/2001 on electronic signatures and its annexes (I and II) issued in compliance with Directive 99/93/EC on electronic signatures.

It should be pointed out that for purposes of completeness and direct relation between double-key certificates, this introduction makes reference to both qualified and non-qualified certificates. For details about qualified certificates please refer to the Qualified Certificates Policy with unique global identifier OID 1.3.6.1.4.1.29402.1.2.1.1.1.1

In particular, the use of two different SMART-SIGN certificates (for two different pairs of cryptographic keys) **totally separates** the use of the subject's advanced electronic signature for "*conscientious signature creation without possibility of its repudiation*" (Non-Repudiation), from **other uses** of electronic signatures (e.g. Web authentication, email signatures, key and data encryption, etc.) whose legal status is limited to that of evidence under the law.

1.1.2 Classes of Personal SMART-SIGN™ Certificates

Personal **SMART-SIGN™ (double key)** certificates are available in different **classes** which determine mainly the scope and amount of the transactions for which they may be used and, therefore, their issuer's maximum limit of liability. Classes are used to classify **SMART-SIGN™** certificates into the different guarantee and pricing policy levels offered which are intended to meet the different transaction needs of their holder in the Information Society.

A pack of personal **SMART-SIGN™ (double key)** certificates contains **always two supplementary certificates of the same class** (one qualified certificate and one authentication certificate).

1.1.3 Key properties of SMART-SIGN™ certificates

ATHEX's personal **SMART-SIGN™ (double key)** certificates are issued only to natural persons or legal representatives of legal persons upon a common application-contract with their issuer (subscription contract) and stored always on the same personalized device together with the relevant pairs of cryptographic keys they certify.

Their co-existence on a common device and the fact that they are based on a common application-contract and supporting documents for their issuance entails **full interaction on their validity**. This means that any action which affects the validity of one certificate in a pair of **SMART-SIGN™ (double key)** certificates, such as for instance activation, cessation, revocation or expiry, will, at the same time, have the same effect on the other certificate.

As a result of the common management of and interdependence between the certificates in a pair of **SMART-SIGN™** certificates, the certificates are subject to (almost) the same policy, which only differs in terms of the limitations in their scope (*see paragraph 2.2 "Certificate applications and use limitations"*) and of some of their technical specifications.

The above scheme ensures that the high level of security and management imposed under applicable legislation and European standards for qualified certificates (so that they can support the signing of electronic documents and have the same validity of handwritten signatures) is at the same time offered to the accompanied authentication certificate, which is **not** issued as qualified (according to the definition in the law) only as specified in the present policy.

1.2 POLICY CHARACTERISTICS AND IDENTITY

1.2.1 Nature of the Non-Qualified Certificate Policy and its relationship with the Certification Practice Statement of Non-Qualified Certificates (C.P.S. N.Q.C.)

The *Non-Qualified Certificate Policy (Q.C.P.)* lays down the main terms for the issuance, management and use as of well as the specifications for a specific type of certificate, **regardless of its issuer.**

Therefore, the certificate policy establishes "***a set of rules which can indicate the suitability of the certificate in a specific community and/or class of applications with common security requirements"*** and is addressed at the same at both the *Certification Service Provider (CSP*), and the certificate holder *(subject)* as well as at third party-recipients *(relying parties)* of that certificate, **and can legally bind and/or operate for the benefit of all parties involved.**

On the other hand the *Certification Practice Statement of Non Qualified Certificates (C.P.S N.Q.C.)* aims to "***establish the organization and operation method and the security practices and rules***" followed by a specific *Certification Service Provider (CSP*) **when it comes to non-qualified certificates.**

In conclusion, the Non-Qualified Certificate Policy establishes "***what*** *rules must be followed*" to issue and manage a specific certificate, while the C.P.S.N.Q.C. establishes "***how*** *the rules will be applied"* by a Certification Service Provider (hereinafter CSP). Therefore, for a CSP to issue a specific certificate the Policy Management Authority of the certificate must have first established compliance of the CSP's C.P.S.N.Q.C. with the requirements of the relevant Certificate Policy for Non-Qualified Certificates.

Note: "*The Policy Management Authority responsible for establishing compliance of a CSP's Certification Practice Statement (even of ATHEX!) with these policies for SMART-SIGN™ Certificates is ATHEX's Policy Management Committee". For more information and contact information refer to the last chapter.*

1.2.2 Text structure and content - Compliance with standards

Text structure is **based** on *IETF RFC 2527 (1999): Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework* and on *IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,* which was replaced by the above IETF RFC 2527.

As regards certificate profile and the Certificate Revocation List (CRL), the algorithms used, use of the fields X.509 - RFC 5280 and the requirements set out in Greek Presidential Decree 150/2001 on electronic signatures and its annexes (I and II) issued in compliance with Directive 99/93/EC on electronic signatures, this policy (as well as the policy for **Qualified Certificates**) adopt the recommendations of *IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF RFC 3739 (2004): Internet X.509 Public Key Infrastructure: Qualified Certificates Profile* and *ETSI TS 101 862 v1.2.1 (2001-06) Qualified certificate profile*.

1.2.3 References and identifiers (OIDs)

This text must be referred to with the title *ATHEX SMART-SIGN™ (double key)–Class 1 Personal Certificate Policy* or using the abbreviated form: **SMART-SIGN –1 PCP**.

In computer applications, as well as in the relevant field in each certificate, these policies will be referred to using ATHEX's globally unique **identifiers (OIDs)**:

1.3.6.1.4.1.29402.1.2.2.1.1.1

for the **SMART-SIGN** - **Class 1**, **Version 1.0 APC Policy**

where:

1.3.6.1.4.1.29402	ATHEX Identifier (OID), registered with IANA
1	ATHEX'S Independent department "Public Certification Services"
2	Certificate Policies
2	Authentication Certificate
1	Certificate Class (1)
1.1	First and second digit of the Practice's version number

2 CERTIFICATE COMMUNITY AND APPLICATIONS

2.1 CERTIFICATE COMMUNITY

2.1.1 Certification Services Provider, Certification Authority (CA) & and Sub-Certification Authorities (Sub-CAs)

A CSP complying with these policies will be operationally supported by at least one *Certificate Generation Service*, one *Registration Authority* (see below), one *Revocation Management & Status Service* (to manage certificate cessation, revocation and/or activation requests), one *Subscriber Device Provision Service* (see below) and one *Dissemination Service* which will disseminate to the public all necessary information.

The Certificate Generation Service (CGS) or Certification Authority (CA) is the **backbone** of the operation of the Certification Services Provider (CSP) and the one to (digitally) sign the certificates and the relevant Lists with suspended or revoked certificates (RCLs). Vis-a-vis third parties, the CA is legally **the same as the CSP,** which issues its own **Certification Practice Statement of Non-Qualified Certificates** (C.P.S. N.Q.C.) and checks its entire Digital Certification Services provision network for compliance with it, **assuming exclusive liability vis-a-vis third parties/recipients who are justified to rely on its certificates.**

Because the pair of cryptographic keys used to electronically sign a qualified certificate (and the respective CRL) received in the SMART-SIGN pack must **not** be also used to sign other types of certificates, the SMART-SIGN CA uses **two different Sub-Certification Authorities** or **Operational Certification Authorities** (Sub-CAs or Operational CAs), holdersof different cryptographic keys, (where one signs the qualified certificate and the other one signs the authentication certificate). However, their certificates are signed by the CSP. Therefore, in the **Issuer** field in SMART-SIGN certificates, the CSP is listed in subfield **O** (=**O**rganization) and the respective Sub-CA is listed in subfield **OU** (=**O**rganization **U**nit).

The certificate of the same Issuer may be **either** *self-signed*, in which case the certificate user/recipient must have installed it on his terminal as **Root Certification Authority** (Root CA), **or** signed by another acceptable Root CA.

2.1.2 Registration Authority

The Registration Authority (RA) is the authority which reviews the applications of natural persons wishing to obtain personal SMART-SIGN certificates for accuracy and completeness. If it **approves** an application it instructs the CA to issue the certificates together with the necessary information should the subscriber choose to have its qualified certificate generated by ATHEX. The Registration Authority may be an **internal function** of the CSP or be outsourced by the latter, in which case the contractor will have specific duties in accordance with this policy and be contractually bound with the CSP.

The Registration Authority works with one or more *Local RA Assistants* (see below) and with the *Subscriber Device Provision Service* (SDPS. See following paragraph) to collect and check the personal data and the corresponding public keys which must be included in the SMART-SIGN certificates (under this Policy and the relevant Certification Practice Statement) before sending them to the CA. It also works with the relevant Revocation Management & Status Service to authenticate subscribers who apply for the suspension or activation of their SMART-SIGN certificates.

The Registration Authority does not itself issue certificates, and therefore is **not** part of the certificate validation chain between the Root CA and natural person being certified. If, however, it is so envisaged in the CSP's CPS, it too may be mentioned in the SMART-SIGN certificates it approved, in an additional subfield with the prefix "OU" in the Issuer field in the following way: OU= RA: *Registration Authority Name*.

2.1.3 Subscriber Device Provision Service (SDPS)

The Subscriber Device Provision Service (SDPS) prepares and provides to approved subscribers (see below) of SMART-SIGN certificates the personalized Secure Signature Creation Devices (e.g. smart cards) required under this policy, where it will create and store appropriate and unique pairs of cryptographic keys. At the same time it will communicate to the Registration Authority the **subject's public keys** created which

must be certified. The SDPS may be an internal department of the CSP or of the Registration Authority it serves, or be outsourced to a contractor who is bound with them by way of contract.

The SDPS personalizes the device intended for an approved subscriber, indicating on it the relevant subject particulars, in accordance with the CPS. At the same time it may also ensure that subscribers are provided the respective readers for the device, if so asked by the subscriber. The technology of Secure Signature Creation Devices must have been approved by the CSP and may **belong** to the SDPS, the CSP or the cooperating Registration Authority, or even to the relevant Local RA Assistant and be **either** owned by the subscriber **or** provided to him for a limited amount of time (depending on the provisions of the CSP's CPS).

2.1.4 Local RA Assistants

Local RA Assistants (LRAAs) offer to that or to the wider public which they address unique access to the CSP's registration and issuance services for personal SMART-SIGN certificates.

Although the CSP can have its own LRAA to directly offer digital certification services to the public, under this policy, LRAAs are usually **collaborating third parties** which enter directly into contracts with the CSP (or with the Registration Authorities working with the CSP and have been authorized to that end) to help **specific or unspecified natural persons** register to obtain personal SMART-SIGN certificates, **either** because the LRAAs wish to use those certificates in their own "closed" telematics applications (as recipients/relying parties) **or** for commercial purposes.

LRAAs supply to candidate subscribers the necessary printed material (application forms, contracts, documentation, etc.) provided by the CSP, sign (as representatives of the CSP) together with subscribers the subscriber applications-contracts after a passing review of the supporting documents, and forward them to the competent Registration Authority for approval. They may at times provide to candidate subscribers **suitable Secure Signature Creation Devices they own**, working together with the relevant SDPS which will personalize them. They either transfer ownership of the devices to the subscribers or grant them the right to possess and use them.

Under their contract with the CSP, LRAAs **bill and collect** from subscribers the **registration and issuance fees** in respect of SMART-SIGN certificates following a separate pricing policy.

2.1.5 Subscriber (certification subject)

Under this policy, subscribers or certification subjects will be **natural persons** who are exclusive holders of digital cryptographic keys suitable to create advanced electronic signatures, which (keys) are stored on a Secure Signature Creation Device and whose signature verification data (public keys) **have already been certified by way of personal SMART-SIGN certificates** by a Certification Services Provider who complies with this policy (of which they are subscribers).

For someone to become a subscriber and holder of personal SMART-SIGN certificates, he must contact a Local RA Assistant (LRAA) in the network of a CSP which complies with this policy, fill out an application form to the relevant Registration Authority, attaching the **identification documents** stipulated in this policy as well as sign the respective **subscriber application-contract** or otherwise **subscription contract**. The application is reviewed for completeness and the supporting documents are reviewed for appropriateness. Next, the application **must be approved** by the respective Registration Authority, which will give the final instruction to the CA to issue the respective certificates. Until receiving the device and the certificates, the applicant will be considered to be a candidate subscriber.

At the same time the subscriber can be a Recipient (or user or third relying party, see immediately below) of the certificates of other subscribers-subjects.

2.1.6 Recipient (or user or relying party)

A certificate recipient **or** user **or** third relying party will be such natural or legal person who, **after having reviewed and verified the validity of a certificate** in accordance with this policy (see section 6.1) and the specific terms of the CPS of the CSP who issued the certificate, **decide,** on their own initiative or

using their automatic applications, whether their certificate offers the security level they desire in order to rely or not on its contents and proceed to a specific action, act or inaction or to acquire justified belief in an event.

A Certificate User (recipient) may well be a subscriber or even a member of the CSP network itself, who, by following the above procedure, will rely or not on the contents of a SMART-SIGN certificate.

2.2 CERTIFICATE APPLICATIONS AND USE LIMITATIONS

2.2.1 Certificate applications

Although certificates are often issued to be used with telematics applications relating to the activities of a LRAA, the technical specifications of those certificates and their policies also their use in other compatible applications (which require authentication certificates and/or qualified certificates to create an electronic signature) **provided** the administrator responsible for those applications **accepts and sets as suitable** these personal certificate policies in the operating requirements and security requirements of his application.

In any case, however, SMART-SIGN certificates are suitable for use by their subscribers-holders in the following applications **by way of suitable and compatible signature creation and verification software**:

Non-qualified certificates can support/alternatively: they can support a number of applications for electronic signatures, which, although do not have the undisputed procedural validity of electronic signatures created by use of a qualified certificate, can, in accordance with the law, still be used **as satisfactory evidence** for the following purposes:

- **to declare and verify the subject's identity,** even through open communication networks when the subject applies for access to electronic signature-compatible information systems *(used instead of a Username and Password combination);*
- **to sign files and data** in electronic forms (e.g. web forms) ensuring that their source is verified and that they have not been tampered with;
- **to encrypt** and **decrypt** other, usually temporary, symmetric encryption keys *(used for direct secure communication between the two systems)*;
- **to perform financial transactions**, namely 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;
- **to sign email messages** (using email management applications, such as for instance MS Outlook Express). However this is so **only** where the CSP supports and the subject has asked for and provided the **indication of his email address** (see paragraph 4.1.1.) on the SMART-SIGN certificate *(and only for using the specific account);*
- **for code signing** purposes to sign files that are 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).

2.2.2 The encryption certificate could also support data encryption (**using the subject's public key) and** decryption (**using the respective private key). However, given that under the certificate policy it is not allowed to recover private keys, the CSP who chooses to offer this add on** must warn the subscriber about the risk of being unable to recover encrypted data **using the public key in the event of loss or any other situation which will not allow him to activate his private key.Limits to the value of transactions using certificates for monetary transactions**

Pursuant to the provisions of this policy for Class 1, SMART-SIGNTM-Class 1 certificates **MAY NOT BE USED BY THE SUBSCRIBER FOR DIRECTR OR INDIRECT FINANCIAL TRANSACTIONS, REGARDLESS OF VALUE.**

More importantly, such certificates may not be used to perform **monetary transactions, that is transactions involving the payment or exchange of monetary amounts or the provision of assets and/or services against payment of money**

SMART-SIGN certificates in this specific Class (Class 1) can be used **solely and exclusively** to sign and/or encrypt **informative** documents (e.g. reports, communications, statements, disclosures, etc.) or to authenticate and control access of their subject to applications not directly related to the payment of direct or indirect fees or of any other consideration for the provision goods or services (e.g. controlled access to libraries, computer networks, free services, etc.)

In all cases where any third party should decide to rely on a SMART-SIGN™ – Class 1 certificate to directly or indirectly transact with the certificate subject, such party **must consider the above prohibition and the CSP's Maximum Limit of Liability for that Class,** which is established in paragraph 3.2.3 of this Policy.

3 OBLIGATIONS, GUARANTEES AND LIABILITY LIMITS

3.1 OBLIGATIONS OF THE PARTIES INVOLVED

3.1.1 Obligations of the Certification Services Provider

A CSP who issues personal SMART-SIGN™ certificates, as well as the parties who work with it under a contract for the provision of certification services (to the extent that is established for each one of them in this Policy and the relevant CPS of the CSP) will have the obligation:

(1) to have secured a **written approval** of compliance their Certification Practice Statement from the Issuance and Management Authority for the Policies of personal SMART-SIGN™ certificates, which is established in paragraph 10.1, following the procedure laid down in paragraph 10.3.2 *Certification Practice Statement Approval* **before** issuing a certificate referring, directly or indirectly, to this policies;

(2) to safeguard the **reliability and security of their infrastructure** complying with the reliability and security requirements in this policy (Chapter 7);

(3) to check and keep during such time period as is established in this policy (paragraph 6.2.3) **their subscribers' identification documents,** their electronic certificates and the entries about changes in the status of their certificates to be used to settle possible disputes;

(4) to **immediately suspend or revoke** SMART-SIGN™ certificates in line with this policy and as specified in the Certification Practice Statement, informing accordingly the certificate holder;

(5) comply with all **procedures and procedure conditions** laid down in this policy, as these are specified in the compliant CSP's Certification Practice Statement;

(6) to inform subscribers and third relying parties **about the terms and conditions for their services**, providing any one of them who so requests **free of charge** through a widely accessible web page **as well as** in printed form: (a) the **Certification Practice Statements**; (b) at least **these Certificate Policies**; (c) the **Subscription Contract** and the **Recipient Contract**; and (d) their **P**KI **D**isclosure **S**tatement (PDS) which will lay down in brief the most important terms and a description of the services provided by the CSP (*using the structure given in the example of Annex B to ETSI TS 101 456*), as well as all previous versions and inform them well ahead of time about any amendments to such documents.

*[Note: Additional informative material on their website, such as for instance examples illustrating the use of electronic signatures, a detailed presentation of the technical features of their products, and references to applicable legislation **are not mandatory** but **are recommended** under this policy]*.

3.1.2 Subscriber - certification subject obligations

Certification subjects (subscribers) in respect of SMART-SIGN™ certificates must:

(1) furnish **accurate identification information** in their applications;

(2) check the **correctness** of such information in the certificate before requesting its initial activation in accordance with paragraph 5.1.4;

(3) use **exclusively the personalized device** provided to them by the CSP's SDPS to activate their private key;

(4) request **the temporary** (**cessation/suspension) or final revocation of their certificates** if they suspect or become aware that their private keys may have become known by third parties, or in any one of the cases listed in the Certification Practice Statement and the Subscription Contract they have signed;

(5) **not** use their certificates with applications or in transactions **expressly prohibited** under this policy or by the CA in the Subscription Contract and/or its Certification Practice Statement;

(6) **not** use their certificates or associated private keys **after their expiry;**

(7) put in place all measures necessary to safeguard the **integrity, secrecy and lawful use** of their private key, device and activation code (PIN).

3.1.3 Certificate third-party recipient - user obligations

A third party who wishes to become recipient of a certificate, **before deciding to rely on such certificate for any reason,** must first:

(1) become informed about **how** electronic signatures and electronic certificates **function and are used** and have read and understood the terms of this Policy, of the Certification Practice Statement and the associated Recipient Agreement of the CSP who issued the SMART-SIGN certificate;

(2) verify that the certificate is **valid** and **not phoney**, in accordance with section 6.1 *Certificate Validity Verification* in this policy and any relevant terms of the CSP, referring to the Suspended and Revoked Certificate Lists (CRLs) indicated by the CSP;

(3) consider in any case the **CSP's maximum limits of liability** indicated in this policy (see paragraph 3.2.3) and the **guarantee limitations** published by the CSP in its Certification Practice Statement and/or the Recipient Contract.

3.2 CSP GUARANTEES, LIABILITY DISCLAIMER AND MAXIMUM LIMIT OF LIABILITY

3.2.1 Guarantees of the Certification Services Provider

The CSP who has issued a certificate **must guarantee** the following to any third party who **reasonably** relies (that is in accordance with the previous paragraph) on that certificate (whether it is a qualified or an authentication certificate):

- at the time of initial activation of the certificate (see paragraph 5.1.4), the **accuracy of all information** contained in the certificate, and the existence of all data required for its issuance, pursuant to its Certification Practice Statement and to this Policy;
- that the **signatory**, whose identity is attested by the CSP in the certificate, at the time of the initial activation of the certificate **was in 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) it provides to subscribers/certified parties **may be used in a supplementary fashion;**
- that it makes every reasonable endeavor to publish the **revocations of the certificates** pursuant to the terms and the procedure laid down in this Policy and specified in its Certification Practice Statement.

3.2.2 Liability Disclaimer - Exceptions

A CSP issuing certificates **may** disclaim its above liabilities:

- if for any malfunction or failure which has caused damage to a CSP subscriber or any third party, there has been no fault on the part of the CSP **or** if it has acted in compliance with the provisions of the Certification Practice Statement and this Policy;
- if the injured party or such other party —outside the CSP's services provision network— has caused the damage by **violating** the terms and conditions of the CSP's Certification Practice Statement and this Policy; **or** if the injured party **caused** the damage in question by acting improperly, inappropriately or illegally;
- if failure on the part of the CSP to comply with the terms of its Certification Practice Statement and of this Policy is due to *force majeure* (e.g. earthquake, power cuts, strikes etc.).

Also, besides where it is otherwise established in this Policy, a CSP issuing SMART-SIGN™ certificates **does not guarantee** or is not responsible for the suitability, quality, lack of errors or fitness of the SMART-SIGN™ certificates for any given purpose.

Lastly, the CSP **may exclude** from the liability it has by issuing SMART-SIGN certificates, all types of direct or consequential damages, such as for instance foregone gains, criminal or disciplinary sanctions or fines, etc.

4 SUBJECT AUTHENTICATION

4.1 SUBJECT NAMING POLICY

4.1.1 Subject personal information indicated in the certificate

Personal SMART-SIGN certificates authenticate the **natural persons** to whom they are issued, indicating **only** the following personal information of the subject:

- Given Name
- Surname
- Initials (3 digits)
- Nationality (country code)
- Full Name (combination of given name, father's name and surname)

and a subject email address (**optional**)

*[Note: Attributes may be assigned to subjects by way of additional **attribute certificates** which are not subject to this policy.]*

4.1.2 Transliteration of names in the Latin alphabet (ELOT 743)

For purposes of compatibility of SMART-SIGN™ certificates with international applications, **all subject information** will be indicated in the certificate fields using **the Latin alphabet** in line with the ELOT 743 standard.

The proper transliteration of the subject's information from Greek to the Latin alphabet will be ensured by using any suitable documents that the subject will furnish (e.g. passport or ID card), otherwise the CSP's services will use the guidelines laid down in the above standard.

4.1.3 Settling subject naming disputes

The CSP must make provision in its Certification Practice Statement for a procedure or way to settle disputes arising in respect of subject naming. This can be part of the responsibilities of the more general Dispute and Complaint Settlement service the CSP must have in place in line with paragraph 9.1.4 of this Policy.

4.2 SUBJECT IDENTITY VERIFICATION

4.2.1 At initial registration

Both the identity and the validity of the subject applying for the issuance of personal SMART-SIGN™ certificates will be verified by way of a **certified copy** of a public identification document to be furnished by the subject as well as by the subject's **signature** on the application form for the issuance of certificates, **which is mandatory** and will be affixed **before a public authority** which will certify the authenticity of the subject's signature.

Alternatively, instead of the verification of the authenticity of the subject's signature, his identity **may also be verified by the competent employee of the LRAA** to whom the original public identification document will be presented. The employee will sign a certification. This procedure will be used only if it is expressly envisaged in the CSP's Certification Practice Statement and if the LRAA has appointed employees for that purpose and has assumed the respective responsibility vis-a-vis the CSP (or the cooperating Registration Authority) by way of the written contract it has entered into with the CSP.

The certified copy of the public identification document which the candidate subscriber must furnish together with its application must be one of the following:

- ID Card.

- Passport.
- Any other equivalent document providing sufficient proof of the subject's identity under the Greek legislation.

The above documents will be cross-checked, confirmed and approved (if complete and correct) by the CSP's Registration Authority.

4.2.2 At the time of the regular renewal of certificates (before they expire or are revoked)

In the case of a regular renewal, where the subscriber **already has a valid personal** SMART-SIGN **certificate** which has not yet expired or been revoked, **no recheck is required** of the subscriber's identity and validity under the above procedure.

The above can be replaced by the subject's electronic signature (using his **qualified** certificate) in an electronic application for renewal to be provided by the CSP, where the subject will **confirm** (or **modify**, as appropriate) his personal information.

4.2.3 At certificate renewal following expiry or revocation

After his certificates have expired or been revoked, the subject which will then become a candidate subscriber must repeat the procedure laid down in paragraph 4.2.1 (just like at the time of his initial registration), except that he does not need to provide a new certified copy of his public identification documents, if the document initially furnished has not expired and if the subscriber indicates in his application the PIN assigned to him at the time of his previous certification.

4.2.4 At the time of applying for suspension or revocation

To verify the subscriber's identity at the time of his application, whether by telephone or over the Internet, for suspension (temporary revocation or cessation) or final revocation of his certificates, a Secret Phrase may be used which the subscriber will indicate to the CSP at the time of his initial application or at a later time.

In particular as regards the application for suspension (temporary revocation), given that it does not lead to the final suspension of the certificates, it can be done over the telephone at which time some of the applicant's personal information is simply checked against the information on the CSP's file, that is without using the subject's Secret Phrase.

In any case, the authentication of a subject applying for the suspension or even the final suspension of his certificates is **satisfactory** if he applies **in writing** (the application will bear the applicant's electronic or handwritten signature) or in person by visiting one of the services of the CSP's network and showing an identification document.

4.2.5 At the time of the application for reactivation (after cessation)

At the time of the application for the reactivation of suspended certificates made over the telephone or the Internet, the Secret Phrase must be used which the subscriber gave either in his initial application or at the time he applied for the temporary revocation (suspension) of a given certificate.

If the subscriber has forgotten the Secret Phrase, the CSP's competent service will first check some of the applicant's personal information against the information it has on file and then it may remind the Secret Phrase over the telephone.

4.3 PROOF OF POSSESSION BY THE SUBJECT OF THE PRIVATE KEY

4.3.1 Key creation on a personalized Secure Signature Creation Device

The pairs of cryptographic keys, whose public keys will be certified in SMART-SIGN certificates for a subject, must be created and stored on a Secure Signature Creation Device provided by the CSP's SDPS. That device will be personalized for that subject. Personalization involves indicating the subject's name and/or PIN on the device and ensuring that the specific keys contained in the device will be certified for the specific subject-subscriber for whom the device has been personalized.

Before that device is sent to the subscriber, the SDPS will enter in it the associated SMART-SIGN certificates as soon as they are issued by the CA.

In addition, the subscriber can choose to generate the pairs of cryptographic keys directly in the device given to him at the time of his registration. Keys are generated through a specifically configured Internet application accessible to the subscriber after his application has been approved.

4.3.2 Sending the Secure Signature Creation Device and the activation code (PIN) to the subscriber

The SDPS ensures that the personalized device and **the code required for its activation** (PIN) are always sent to the subscriber in separate shipments.

In particular, the device may be sent by mail (to the address indicated by the subscriber in his application) or delivered to the subscriber through the respective LRAA always with proof of delivery. The device activation code (PIN) is always sent in a sealed and opaque envelope to the subscriber's address.

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 same application.

4.3.3 Suspension of certificates until Initial Activation

Immediately after being issued, personal SMART-SIGN™ certificates are assigned a Suspended status (temporary revocation) for security purposes until their Initial Activation (see paragraph 5.1.4). The suspension ensures that, before the SMART-SIGN certificates can be used for the first time, the associated device (and the signature creation data it contains) and its associated activation code (PIN) are in the subscriber's hands.

Moreover, where the Certificates are created by the subscriber, the certificates are activated directly from the specially designed web application. At the same time, the activation code is provided to the subscriber by that application during the key generation procedure.

5 TERMS FOR THE MANAGEMENT OF THE CERTIFICATE LIFE CYCLE

5.1 APPLICATION, ISSUANCE AND ACTIVATION

5.1.1 Subject application and application approval procedure

A candidate subscriber can apply for obtaining personal SMART-SIGN™ certificates through a Local RA Assistant (LRAA) which has entered into a contract with the CSP. The application must include the following:

- the particulars of the subject to be certified (given name, surname, initials, nationality, and one email address (optional));
- the type and particulars (issuer, number, issuance date, expiry date) of the valid public identification document whose certified copy is attached (see paragraph 4.2.1) which demonstrates the subject's personal information listed above;
- the candidate subscriber's contact telephone number and address (where the device, the PIN and any tax documents can be sent);
- an email address, regardless of whether the subscriber applies for the certification of that email address, and/or a fax number where the subscriber can receive in a timely and valid manner information messages (e.g. certificate expiry alert and application form for certificate renewal) sent by the CSP;
- certificate attesting to the authenticity of the applicant's signature issued by a public authority or the competent LRAA employee. As regards certification by a LRAA employee the conditions provided for to that end must be satisfied (see paragraph 4.2.1).

The competent LRAA employee will first carry out a passing check of the application for completeness (in accordance with the above), **co-sign it** and send it (together with the Subscription Contract signed by the candidate subscriber and with the supporting documents provided by the candidate subscriber), in a sealed envelope to the relevant Registration Authority **within a reasonable time frame.**.

Being responsible for the **final check** of the application, the Registration Authority will approve **or** reject the application **or** ask the applicant to provide any missing items **no later than five (5) business days** from the day on which it received the application.

5.1.2 Device personalization and creation of the pair of keys

If the Registration Authority accepts the candidate subscriber's application, the Registration Authority will instruct the SDPS to personalize and provide a device to the subject, giving the SDPS the information required for the personalization.

The SDPS will personalize the device and include the device PIN in a **sealed envelope** for the subscriber and then inform the Registration Authority about the public keys created for that device. Next, the Registration Authority combine the public keys of the subject it received from the SDPS with the information of the subject that is to be certified and sends the respective **instruction** to the CA.

Alternatively, the Registration Authority will deliver to the subscriber a non-personalized device. Then the subscriber will use the specifically configured Internet application to personalize and generate the pair of keys directly on the device.

5.1.3 Issuance of certificates and shipment to the subscriber

When an electronically signed instruction to issue certificates is given by the Registration Authority to the CA, the latter will **issue the electronic SMART-SIGN™** certificates (through its respective Sub-CAs, see paragraph 2.1.1) and have copies sent to the SDPS to store them in the personalized device to be sent to the subscriber, in accordance with paragraph 4.3.2.

Immediately after the certificates have been issued, the CA, together with the Revocation Management & Status Service, will publish their serial numbers in the Certificate Revocation List (CRL) as suspended (temporarily revoked), until they are reactivated (=their suspension is lifted) in line with the following procedure.

Where a Certificate has been issued by the subscriber using the specially configured Internet application, the CRL will be updated automatically by that application without there being need for the SDPS to take any action.

5.1.4 Initial Activation of Certificates

When a subscriber receives the personalized device (with the signature creation data and the suspended certificates)and the respective activation code (PIN), he must **before using them** check that the certificates contained in the device are correct, and, if yes, ask for the Initial Activation, which will result in the **serial numbers of the suspended certificates being deleted from the CRL** so that those certificates can be **reasonably** used by third parties as well.

The Initial Activation is carried out by the CSP's Revocation Management & Status Service after it has received the necessary evidence that the signature creation device, the private keys and their activation code (PIN) have reached the subscriber.

The device delivered to the subscriber must come with written instructions about the importance of and procedure for the initial activation.

In addition, the Initial Activation may be performed via the specially configured web application through which the subject manages the qualified certificate.

5.2 VALIDITY, EXPIRY AND RENEWAL

5.2.1 Certificate validity period

Personal SMART-SIGN™ certificates are valid for **one year** (this period may be extended for up to an additional month for management reasons, which are described in the Certification Practice Statement of Non Qualified Certificates with OID 1.3.6.1.4.1.29402.1.2.1.1) counting from the date of their issue, except for cases of regular renewal (see below) where the validity of the certificates starts immediately after the expiry of a valid certificate.

During the period of validity of certificates, their subscriber may **use them for an unlimited number of times** at no additional charge, in accordance with the terms of this document.

5.2.2 Expiry of Certificates

The dates on which the validity of certificates starts and ends are electronically indicated in them (in line with the X.509 - RFC 5280 standard), and can therefore be **automatically** recognized by most computer applications (which will not allow their use or display a message where an attempt is made to use the certificates outside their validity period.) However, it must be **expressly** stated that after a certificate has expired **the subscriber or any other person must refrain from any** f the signature creation data corresponding to it.

The CSP **may not be held liable** to any third party who relied on certificate that had expired on the date on which the signature was created.

5.2.3 Certificate Renewal

Renewal of SMART-SIGN™ certificates may be either **regular**, where the subscriber asks of the CSP to issue new certificates before his existing certificates expire or are revoked by filling in and electronically signing the renewal application, or **exceptional** (if the certificates have expired or been revoked), in which case the subscriber must repeat the initial registration procedure in accordance with paragraph 4.2.3.

To make regular renewal easier, the CSP will inform the subscriber **at least 20 days before his certificates expire** about the procedure and web address where the subscriber can find the electronic renewal

form, or, if the subscriber has given an email address, will send him an email with the information and the renewal form which the subscriber will fill in and sign.

Certificate renewal involves the issuance of a **new certificate** to the same natural person. That new certificate will become valid on the expiry date of the previous certificate being renewed.

Renewal requires the creation of **new signature creation data** on a new or even the same Secure Signature Creation Device, depending on the CSP's Certification Practice Statement (and provided that the device technology supports the creation of new keys on it).

The CSP may also include additional conditions in the Certification Practice Statement or the Subscription Contract for the acceptance of a certificate renewal application, e.g. it may require approval of the renewal by the LRAA which co-signed the subscriber's initial application, in particular if it is required that if a new device is to be used, then that must come from the LRAA.

SMART-SIGN certificate renewal involves issuing new certificates subject to these policies or to **any recent revised editions of these policies** (see section 10.2) provided that the subscriber has been informed about it. Subject to approval by the respective LRAA, or without that approval if not required by the CSP, the subscriber may, at the time of renewal of his SMART-SIGN™ – Class 1 certificates request their **replacement with SMART-SIGN™ certificates** of **another class**, provided that at the time those such other certificates are provided by the specific CSP.

In addition, the subscriber may also renew his certificate using the specifically configured Internet application.

5.3 SUSPENSION, REVOCATION AND (RE)ACTIVATION

5.3.1 Certificate Suspension And Revocation

SMART-SIGN certificates are **suspended** (temporary revocation) and **revoked** (definite revocation) by publication of their serial numbers in the respective CRL of the CSP.

Certificate suspension **must** originate from the subscriber-holder of the certificates or the CSP in the even that there is the slightest suspicion that the respective signature creation data have become known by any third party. On the other hand, certificates are revoked where there is serious suspicion or certainty about a similar event. The supplier **must** also request the **suspension** of his certificates if he has lost control over the signature creation data or noticed that any piece of information in them is not accurate.

The CSP may suspend or revoke certificates, and inform the subscriber about it, at any time if it believes that this will protect the security of its infrastructure or in any other case envisaged in its Certification Practice Statement. Where certificates are revoked at no fault on the part of the subscriber, the CSP must indemnify the subscriber for the remaining portion of the validity period of his certificates (see paragraph 9.2.2).

SMART-SIGN certificates **may not** remain in Suspended status for an uninterrupted period of over one week; if by the end of that period the reasons which caused the suspension of the certificates have not been resolved so that they can be (re)activated, the certificates are **automatically** definitely revoked!

Lastly, the subscriber may also suspend or revoke his certificate using the specifically configured Internet application. The application will automatically publish the serial numbers of those certificates on the CSP's CRL.

5.3.2 Activation after suspension

Certificate (re)activation after their temporary suspension involves deleting their serial numbers from the CRL where they had been published when the certificates were suspended.

For certificates to be activated the subscriber-holder of the certificates must apply for it, whereby he **will assume full responsibility** for the non-existence of reasons which would case the certificates to be definitely revoked. By relying on reasons of security of its infrastructures or such other reasons as are

envisaged in its Certification Practice Statement, the CSP **may**, however, **decline the request** for the (re)activation of the subscriber's certificates and definitely revoke them.

In addition, a subscriber may reactivate his certificate using the specifically configured Internet application for certificate management. During this procedure, the serial numbers entered on the CRL during the suspension procedure will be removed from it automatically by that Internet application.

In no case may definitely revoked certificates be (re)activated!

5.4 CERTIFICATION STATUS DISSEMINATION SERVICES

5.4.1 Issued Certificates Directory Service

A CSP that issues SMART-SIGN certificates **must** make available on a specific and well-known Internet address a directory of certificates issued, where it will publish and make accessible to all interested third parties all personal SMART-SIGN certificates it has issued (both qualified and authentication certificates) for verification, **provided that** the CSP subscriber and holder of those certificates has not opposed to that publication at the time of applying for their issuance or at a later time *(see paragraph 9.1.3: Personal Data Protection).*

Certificates may be published using LDAP or HTTP technology. Their publication will allow searching for specific certificates on the basis of the subject information included in them or certificate serial numbers. It is permitted that that directory should also include other SMART-SIGN certificates which are not active at the time (due for instance to expiry or revocation). In this case, however, the validity status of the certificates displayed must be clearly indicated.

This service **must** (insofar as there is a second backup system allowing it) be available around the clock and every day of the year, immediately updated (no later than in 24 hours) after each certificate is issued, revoked and/or activated and provided **free of charge** by the CSP.

5.4.2 Suspended and Revoked Certificate List (CRL) Service

The list with the SMART-SIGN certificates which the CSP has suspended or revoked (Certificate Revocation List - CRL) must be available and provided free of charge around the clock every day of the year (insofar as there is a second backup system allowing it) **on the CSP's Internet address indicated by the CSP on the SMART-SIGN certificates at the time of their issuance** (in the required CRLDistributionPoint field).

The CRL must be displayed based on the LDAP (in line with section 8.2 on the CRL Profile). The CRL must as a minimum include fields for the certificate serial number indicated, indicators showing the reason why a given certificate was placed on the list (e.g. suspension or definite revocation, etc.) and the exact time the entry was made in it. All data must be protected against tampering by way of the Ca's **electronic signature** using the very same keys it used to issue the certificates on the list!

The list **must be renewed at least every 24 hours** (when a new time-stamped list will be issued indicating the exact time of the next scheduled version). The CSP may envisage in its Certification Practice Statement cases in which it will issue unscheduled versions of the CRL.

Other ways of publishing the list of certificates, including by using the On-line Certificate Status Protocol (OCSP) or by issuing partial lists (delict), are allowed provided they are expressly envisaged in the CSP's Certification Practice Statement.

6 VALIDITY AND PROBATORY VALUE

6.1 CERTIFICATE & SIGNED DOCUMENT VALIDITY CHECK

6.1.1 Personal SMART-SIGN™ Certificate Validity Check

For a SMART-SIGN certificate to be used or for someone to reasonably rely on them, their **validity** must be checked and confirmed **first**.

Valid SMART-SIGN certificates are certificates whose expiry date has not passed or which have not been revoked definitely or temporarily (suspended).

A SMART-SIGN certificate is checked for revocation by **checking** its serial number —which is unique for it and included in it as a field— against the serial number of the certificate included in the CRL published by its CA in line with paragraph 5.4.2 of this policy.

This can be checked **either** directly by the interested party, by reviewing the CRL and checking the serial number as described above, **or** by using a special software which checks certificates for validity (suitable for checking CRLs) and which **the user trusts**.

6.1.2 Installation and validity check of the chain of certificates higher in the hierarchy

SMART-SIGN certificates must be signed by one Sub-CA (see paragraph 2.2.1) which in turn must have a certificate signed by the main CA representing the CSP.

In this manner, besides the above validity check of SMART-SIGN certificates, the third party relying on them must also install on his computer and check both the Sub-Ca's certificates as well as those of the main CA **to rule out any case of phoney certificates**.

The certificate chain that must be checked stops with a **self-signed** certificate, that is a certificate where the Issuer and the Subject fields are exactly the same and which the user **must accept and install** as Root-CA on his computer.

The CSP **must** provide on all of its web pages **all certificates** necessary for checking the trust chain of certificates (from the Root-CA to the final SMART-SIGN certificates).

6.1.3 Long-term check on signed documents - Time stamping

To safely demonstrate the validity of a document signed by way of SMART-SIGN certificate valid at the time of signing, **after the expiry or revocation of such certificate** (long-term check), **time-stamps** must be included in that document **before** the expiry or revocation of the certificate used.

This is the only way to ensure that the document was not falsely signed by a third party to whom the signature creation data were exposed **after** the expiry of the validity of the certificate (which could have also been revoked due to such exposure of the data!)

Time stamping services, which are not the subject of this policy, could be provided by the same CSP who complies with this Policy and issues SMART-SIGN certificates or by any other CSP.

6.2 INFORMATION ENTERED - ACCESS - ARCHIVING DURATION

6.2.1 Evidence entered during certificate management

A CSP issuing SMART-SIGN certificates **must** keep a personal file for each subscriber. Such file will contain at least the following information:

(a) the initial application together with the signed contract and the supporting documents attached to it;

(b) the approval report for the subscriber's application, signed by the competent employee of the Registration Authority, or other relevant proof;

(c) the report regarding the preparation of the Secure Signature Creation Device, indicating the details of the personalized device of the subscriber and proof of its sending to and receipt by the subscriber, signed by the competent employee of the Subscriber Device Provision Service, or other relevant proof;

(d) the report regarding the issuance of the SMART-SIGN certificates indicating their serial numbers, the exact time of issuance and the certified public keys, as well as making reference to the act and to the exact time the certificates were placed under initial suspension, signed by the competent employee of the CA, or other relevant proof;

(e) information and evidence for all other change of status request for the subscriber's certificates (such as initial activation, suspension, activation, or revocation), clearly indicating who, how, when those requests were made and if and when they were satisfied;

(g) reports for each regular certificate renewal, making reference to the subscriber's signed renewal instruction, or again the information under (a), (b), (c) and (d) for each exceptional renewal;

(h) information and any copies of documents regarding complaints or requests for dispute settlement arising out of or in relation to the subscriber, as well as information about the progress of the settlement.

The CSP **may** keep part of the above information in **electronic format** (logs), on condition that it can ensure its integrity and availability, provided however that such logs can be printed on paper in intelligible language, be certified by the CSP and made available to inquiry procedures **whenever required**.

In addition to subscriber information, the CSP must log and be able to prove the exact times and contents of all versions of the CRLs it has issued.

6.2.2 Archiving period

All of the above information that relate to the existence and validity of a SMART-SIGN™ certificate **will be kept unaltered for 30 years** from the expiry of the certificate so that it can be available to the Dispute Settlement procedure provided by the CSP (see paragraph 9.1.4) and to serve as evidence in any other legal or administrative procedures.

This possibility **will not be guaranteed** to any subscriber-certified party or any other party who has relied on a certificate **after that period.**

6.2.3 Access to evidence

Direct access to information on the file will be given to the subscriber. **Indirect** access (through a Dispute Settlement Committee) to the information will be given to any third party who has a legitimate interest related to a specific certificate of a subscriber.

If the Dispute Settlement or Complaint Handling Procedure which the **CSP must envisage and make available** (in line with this Policy) to third parties or its subscribers fails to satisfied an interested party, the CSP must produce the above evidence to any judicial or administrative authority responsible for handling the dispute when so requested by such authority.

7 SECURITY & RELIABILITY REQUIREMENTS

7.1 TECHNICAL REQUIREMENTS FOR SECURITY

7.1.1 CA cryptographic keys

The cryptographic keys of the Root-CA and of his Sub-CAs (who sing the SMART-SIGN™certificates) must be created and stored using a **Hardware Security Module** whose function will be certified under FIPS 140-2 level 3.

At least two (2) accredited persons must cooperate for the creation, use, copying, storage and recovery of the above keys.

The size of the Ca's keys must be no less than **2048 Bits** and the size of those of the Subordinate CAs must be no less than **1024 Bits.** The Livest - Smartphone - Telematics Algorithm **(RSA)** must be used for their creation and the Secure Hashing Algorithm – 1 **(SHA-256)** must be used for their hashing at the time of signing.

Use of the keys of the Sub-CAs of a CSP who complies with this policy must be limited **solely and exclusively** to the signing of Certificates and CRLs. Their use for any other purpose or usage will be prohibited.

The cryptographic keys of the CA (and more often of its Sub-CAs) must have a limited validity period (no more than 20 years for the CA and no more than 10 years for the Sub-CAs). When they expire (or even revoked) they must be destroyed as soon as new keys have been created to replace them.

7.1.2 Cryptographic Keys and Secure Signature Creation Device for the private keys of subscribers.

The keys of subscribers must be created by the CSP's SDPS. Security levels equivalent to those ensured for the keys of CAs must be ensured during their creation. Public keys produced for the subscriber by the SDPS to be certified by way of SMART-SIGN™ certificates must be **no less than 2048 Bits** and use the same algorithms for their creation, the creation of the signature and hashing (RSA and SHA-256 respectively).

The personalized Secure Signature Creation Device (e.g. smart card) which must be provided to the subscriber of SMART-SIGN™ certificates through the CSP's SDPS must comply with the standards that apply each time and require the use of the secret **Activation Code** (PIN) for using the private keys it contains. The CSP shall ensure that the PIN is only communicated to the subscriber.

7.1.3 Escrow or other private key recovery procedure

The signature creation data (*private keys*) which are created by the CSP's SDPS for a subscriber whose signature verification data (*public keys*) will be certified by way of SMART-SIGN certificates, and the CSP private key **may not** be extracted from the subscriber's personalized device or copied in any file of the CSP, **nor** be subjected to any other method which allows, even on conditions, their **recovery**, such as key escrowing.

7.2 OTHER CSP SECURITY AND RELIABILITY REQUIREMENTS

7.2.1 CSP System Reliability - Compliance with international security standards

A Certification Services Provider (CSP) who issues SMART-SIGN™ certificates under this policy must have ensured a reliable system to provide its services. Such system must fully comply with Greek Presidential Decree 150/2001 on electronic signatures and its annexes (I and II) issued in compliance with Directive 99/93/EC on electronic signatures. In addition, it must have ensured a reliable system to provide its services which must be in line with *IETF RFC 2459 (1999): Internet X.509 Public Key Infrastructure – Certificate and CRL Profile* and *CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures* of the European Committee for Standardization (CEN).

7.2.2 Physical Security, Procedure Security, Staff Training and Reliability Check

The CSP must take all measures necessary to ensure the physical security of the systems it operates, such as ensure air-conditioning, uninterrupted power supply, lack of leaks, fire protection and prohibition of physical access of unauthorized persons to the main operational area of its system.

At the same time, it must have clearly established in its Certification Practice Statement procedures which ensure that the system is operated by authorized persons with specific roles and access rights, requiring that two users should cooperate for critical operations.

Lastly, it must ensure the constant training and informing of its staff, as well as ensure, through contractual requirements and checks, the confidentiality and non-disclosure of sensitive security information regarding the system and personal data of subscribers.

7.2.3 CSP financial reliability and sustainability

A CSP issuing SMART-SIGN™ certificates **must be a legal person** (governed by private or public law) and offer suitable guarantees for its financial capacity and sustainability, which is necessary for the long-term performance of digital certification activities. In any case, a CSP that complies with this Policy **must envisage in its Certification Practice Statement** the actions that must be taken and the way files and active certificates must be handled in the event that its operation cease or stop.

Civil liability insurance taken out by the CSP with a reliable insurance organization in respect of the digital certification services it provides **is recommended but not mandatory for this class** (Class 1) of SMART-SIGN™ certificates, as those certificates may not be used in financial transactions and, therefore, the CSP assumes a low level of maximum liability in respect of their issuance. Where there is no satisfactory civil liability insurance, if the CSP is a society Lancom (SA) or limited liability company (LTD), it must have a share capital of no less than one million two hundred thousand Eurostat (EUR 1,200,000).

7.2.4 Operational independence

If the provision of digital certification services is part of the overall activities of the legal person who acts as a CSP, the department dealing with these activities **must operate completely independently and have separate infrastructure and facilities** from the rest of its departments.

7.2.5 Voluntary Accreditation

A Certification Services Provider (CSP) issuing SMART-SIGN™ certificates shall be **subject to** voluntary accreditation by the National Telecommunications and Post Commission (EETT) or equivalent European voluntary accreditation organization.

The above condition must be satisfied no later than in one (1) year from the publication of the respective voluntary accreditation regulation by EETT.

8 CERTIFICATE PROFILE & CRL

8.1 CERTIFICATE PROFILE

8.1.1 Type and Version Number

ATHEX's Smart-Sign™ certificates must be X.509, Version 3 (Version 3), which support the use of *extensions*. The version number always refers to the relevant field of the certificate.

8.1.2 Content and Meaning of Certificate Fields

Smart-Sign™ certificates (qualified or authentication certificates) contain at least the following X.509 V3 basic and extended fields:

Field Name (*)	Content	Remarks
Version	"V3"	*Version '3' of online certificate 'X.509 - RFC 5280 CRL' supports extended fields*
Serial Number	[Integer]	*Unique number of the certificate generated by the specific CA*
Signature Algorithm	[Identifier]	*Specifies the algorithm used for hashing and signing the certificate*
Issuer	(**Distinguished Name (DN)** type X.501 for the Issuer)	*The name of the CA, broken down in sub-fields. See analysis in paragraph 8.1.4 below*
Valid From	[Date]	*The certificate issuance date.*
Valid To	[Date]	*The certificate expiry date.*
Subject	(**Distinguished Name (DN)** type 'X.501' for the Subscriber)	*The subscriber-subject name, broken down in X.501 subfields with the properties established in the X.520 standard.* *The subfields used and their contents are detailed in paragraph 8.1.5 below*
Public Key	[Hexadecimal number]	*The certified Public Key of the Subscriber (subject)*
CRL Distribution Points	*(In the subfield 'Distribution Point Name:/Full Name:=')* [Address type 'URI']	*The address where the recent Certificate Revocation List (CRL) is published*
Certificate Policies	[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	Non Repudiation, or + Key Enchipherment + Data Enchipherment	*It determines the permissible uses of the subscriber's private key depending on the type of the certificate*

(POINT 5)

(*) = *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, it must be an option for Smart-Sign certificates to have additional fields providing more information, e.g. text-statements about the particular terms of use (e.g. maximum limit of permitted transactions) of the certificate or identifiers of the keys used.

8.1.3 Form and Content of Distinguished Names (Dn)

Distinguished names DNs) that are contained in the Issuer and Subject fields of Smart-Sign™ certificates must be in the form of ITU-T Recommendation X.501 -Name, which contains subfields with specific attributes. Such attributes (such as Given Name, Surname, Country, etc.) are detailed in ITU-T Recommendation 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] see paragraph 4.1.3) for international compatibility.

8.1.4 Distinguished name (DN) of the Certificate Issuer

The Distinguished Name (DN) in the Issuer field in Smart-Sign certificates, which determines the certificate Issuer, must contain the following information:

Subfield	Explanation	Content
O=	***Organization***	name of the CA (CSP)
OU=	***Organization Unit***	Name of the Sub-CA *(it should be indicated if it is intended for qualified or non-qualified certificates)*
[… OU=]	***Organization Unit [additional]***	Additional identifiers of the CA *[Optional]*
CN=	***Common Name***	Common name of CA and Sub-CA
C=	***Country***	Code of the Ca's country *(2 letters)*

8.1.5 Distinguished Name (DN) of the Subscribers (Subject)

The Distinguished Name (DN) in the Subscriber (Subject) field in Smart-Sign™ certificates (see paragraphs 4.1.1 - 4.1.3) must contain the following information:

Subfield	Explanation	Content
GN=	***(Given Name)***	Subscriber's name *(in full or initials)*
S=	***Surname***	Subscriber's surname
I=	***Initials***	Subscriber's initials *(1-3 first letters)*
CN=	***Common Name***	Combination of Given Name - Initials- Surname
SN=	***Serial Number***	Subscriber personal identification code *(Unique code of the Subscriber with the CA)*
E=	***E-Mail***	Subscriber's e-mail address *(in RFC 822 Name format) - [Optional]*
C=	***Country***	Code of subscriber's country of nationality *(2 letters)*

8.1.6 Critical fields

A **critical field** in Smart-Sign™ certificates, a field which must be recognized and interpreted by any application before accepting and using the contents of the certificate, is **just the Key Usage field** which by its codified contents determines the type and general uses of the certificate.

This is done by assigning its *Critical Flag* subfield to *True*.

8.2 CERTIFICATE REVOCATION LIST (CRL) PROFILE

8.2.1 Type and Version Number

CSPs who comply with these policies must issue X.509, CRL Version 2 CRLs. This version supports the use of *extensions*. The version number always refers to the relevant field of the certificate.

8.2.2 Content and Meaning of CRL Fields

The Certificate Revocation Lists (CRLs) issued by a CSP in respect of Smart-Sign™ certificates issued by its Sub-CAs must contain the following fields:

Field Name	Required	Content	Remarks
Version	YES	"V2"	*Version '2' of standard 'X.509 - RFC 5280 CRL' supports extensions.*
CRL Number	YES	[Integer]	*Unique number identifying a CRL for a given Sub-CA.*
Signature Algorithm	YES	[Identifier]	*Specifies the algorithm used for the hashing and signing of the list.*
Issuer	YES	(**Distinguished Name (DN)** type X.501 for the Issuer)	*The name of the Sub-CA (who signs the CRL) analyzed into sub-fields.* See paragraph *8.1.4*
This Update	YES	[Date]	*The issue date and time of the current CRL update.*
Next Update	YES	[Date]	*The date and time of the next scheduled CRL issue.*
Authority Key Identifier	NO	[Integer]	*Identifies which of the Issuer's key pair corresponds to specific CRL (from which it was signed).*
Revoked Certificates	YES	[Certificate List]	*The updated master list with information regarding revoked certificates up to the CRL issue. Smart-Sign (See table below).*

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

Field Name	Required	Content	Remarks
User Certificate	YES	[Integer]	*The unique serial number of the Smart-*Sign certificate *revoked*
Revocation Date	YES	[Date]	*The date and time of CRL issue with which this certificate was revoked.*
Reason Code	YES	(Byte with indications on the ground that this certificate was revoked - according to RFC 5280 or the relevant standards in force)	*Identifies the reason for revoking the certificate e.g. revocation due to key exposure or simple cessation (temporary revocation)*
Invalidity Date	Optional	[Date]	*The date and time of the certificate's revocation request.*

8.2.3 Critical fields

CRLs issued for Smart-Sign™ certificates there is no need for critical field.

9 OTHER GENERAL CONDITIONS

9.1 RIGHTS AND PROTECTION

9.1.1 Intellectual property 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 SSL Certification Practice Statement by third parties without written permission **is expressly prohibited**.

9.1.2 Trademarks and other properties

SMART-SIGN™ is a registered trademark of ATHEX SA and its use by any third party for related products or services is strictly prohibited.

Only Certification Services Providers (CSPs) who have been approved by ATHEX's Policy Management Committee under paragraph 10.3.3. and have received **written permission** for that will be entitled to claim that their certification services are compatible with the provisions of these Personal Certificate Policies for ATHEX's SMART-SIGN™ *(double key)* – Class 1 certificates.

9.1.3 Personal Data Protection

Due to its nature, the provision of digital certification services is directly linked to the processing and dissemination of the personal data of the subjects certified.

Therefore, CSP's issuing SMART-SIGN™ certificates must, under this policy, comply with Law 2472/97 *on the protection of individuals with regard to processing of personal data*, as in force and also undertake:

(a) to **refrain from publishing** in the public directory of certificates other personal data of the subscriber the CSP may be in possession of, save the information of the subjects certified (based on the approved application-contract) and the information indicated in the certificates;

(b) to **offer the possibility** to subscribers, both at the time of his application for the initial issuance of certificates and at any such later time the subscribers may decide, **to request the non-publication** of their certificates in the public directory of active certificates kept by the CSP;

(c) to disclose other personal data of subjects of SMART-SIGN™ certificates to third parties only for the **settlement of disputes** arising out of the use of a specific certificate, unless the subject has otherwise expressly consented.

9.1.4 Dispute Settlement and Complaint Handling Policy

A Certification Services Provider issuing SMART-SIGN™ certificates must have ensured a dispute settlement and complaint handling procedure for the subscribers and the recipients of its certificates who wish to settle their disputes with and/or complaints towards it out of court.

The procedure must establish a time frame of **no longer than one (1) month** from the interested party's written request, during which the CSP's competent committee must respond. That committee must comprise at least three members and include one administrative officer, one system security officer and one of the company's legal advisers.

Those services **must be provided free of charge to the interested party**, at least where that party does not bring the case before the courts during that period of time.

9.2 PRICING POLICY

9.2.1 Pricing Policy Publication

A compliant CSP may, if it so wishes, to set and publish a pricing policy for the SMART-SIGN™ certificates it offers, **hence establishing a maximum level** for the pricing policy of the LRAAs in its network.

As for the rest, LRAAs may have in place a separate pricing policy for the CSP services they offer to their subscribers.

The pricing policy must establish the billing method for registration fees and issuance and renewal fees in respect of SMART-SIGN™ certificates as well as for the Secure Signature Creation Devices and any readers offered to subscribers.

Services linked to the Directory of issued Smart-Sign™ certificates and CRL publication services, as well as SMART-SIGN™ revocation, suspension and activation services **must be offered free of charge.**

9.2.2 Subscription Fee Refunds

Registration and issuance fees in respect of SMART-SIGN™ certificates a candidate subscriber may have paid at the time of his application **must be refunded** to the applicant (by the person who received them) if the Registration Authority did not approve the applicant's application.

Provision must also be made for the refund by the CSP to the subscriber of issuance fees (but not registration fees) should the CSP revoke the subscriber's certificates for no fault of the subscriber. In this case, the issuance fees corresponding to the time remaining until the normal expiry of the suspended certificates must be refunded.

9.3 CONSTRUAL AND ENFORCEABILITY

9.3.1 Authentic construal of the terms hereof in comparative evaluations

In cases of comparative evaluation of these Policies (*with Certification Practice Statements to assess their compliance or with other Certificate Policies to determine their equivalence or compatibility in line paragraphs 10.3.1 and 10.3.2 of this Policy*) for the purpose of establishing commercial partnerships in the public certification service provision market, ATHEX's Policy Management Committee **will be the only one responsible** to authentically construe the terms of this Policy and thus reach or not conclusions regarding this policy compared with other texts.

9.3.2 Enforcing-Maintaining Void Terms

This policy which applies to **non-qualified SMART-SIGN™ – Class 1 certificates** is binding on the parties of the community of SMART-SIGN™ certificates (CSPs and third parties, subscribers and recipients involved in the provision of the services) which incorporate this entire Policy in the respective contracts by mere reference to it**.**

Where there is a conflict between this Policy and any term in such contracts, **this Policy will have precedence**.

Where a provision or paragraph in this text is **unenforceable** or **void** this will not cause the entire or any other portion of this Policy unenforceable in respect of personal SMART-SIGN™ – Class 1 certificates, and this Policy will be considered to have been amended by deletion of or amendment to such provision so as to become **valid and enforceable and**, to the extent possible, **compliant with its initial purpose**.

9.3.3 Applicable law and competent courts

This Policy **is governed by Greek Law** and **the Courts of Athens will have jurisdiction** over any action, contestation or dispute in relation to it. The contracting parties hereto will hereby be subject to the accessory jurisdiction of such courts, and incorporate this Policy by mere reference to it in the contracts they make between them.

10 POLICY MANAGEMENT AND REVISION

10.1 ISSUANCE AND MANAGEMENT AUTHORITY

10.1.1 Name - Duties - Obligations

ATHEX's **Policy Management Committee** will be responsible for the issuance and management of this policy on personal SMART-SIGN™ certificates.

This Committee will be the **supreme body** responsible for ATHEX's Digital Certification Services in matters of policy shaping and security levels for the certificates issued as well for developing a strategy to harmonize ATHEX's certification services with the required legal and technical specifications and market trends. This Committee will be **set up** by ATHEX's Digital Certification Services and **include** senior management officers, technicians and security managers as well as legal advisers of ATHEX SA.

The Policy Management Committee will be responsible for the **issuance, publication and revision** of the Certificate Policies issued by ATHEX's Digital Certification Services and for **the approval** of its Certification Practice Statement as compliant with the requirements and specifications laid down in its Policies.

In addition, this Committee will be the only one responsible for the legal and technical processing and **approval (***following comparative evaluation against the Policies it issues, see section 10.3*) of other Certificate Policies and Certification Practice Statements in the event that ATHEX's Digital Certification Services work **with other certification services providers or certification authorities** (e.g. *cross-certifying, adoption or policy-mapping*).

The Committee will meet every month to supervise compliance with its policies, consider the need to revise the policies or issue new ones and carry out construal and comparative evaluation activities, when required.

10.1.2 Contact Information

The Policy Management Committee's offices are housed at the premises of ATHEX SA and any questions, remarks or comments to the Committee must be sent to:

ATHEX SA

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/web/guest/digital-certificates

10.2 POLICY REVISION

10.2.1 Submission, approval and publication of revised versions

ATHEX's Policy Management Committee will decide whether it is necessary or not to revise these Policies on SMART-SIGN™ certificates **either** on its own initiative following amendments to applicable legislation or technical standards on electronic signatures **or** acting on a question or request made by ATHEX's Digital Certification Services and its partners who are subject to these Policies.

The necessary revisions of these Policies are prepared by members of the Committee and finalized **only by approval** of the new text by all members of the Committee **and by its publication** on the respective

web page of ATHEX's Digital Certification Services (http://www.athexgroup.gr/el/web/guest/digital-certificates-pki-regulations) **at least ten (10) days before it becomes effective**.

All approved revisions must include an Introduction chapter summarizing the amendments made to the Policies as compared to their initial version, and previous versions **must continue being published** as such on the same web page.

10.2.2 Criticality and numbering of revised versions

Critical revisions of this Policies will be such revisions as substantially change or affect the relations (rights and obligations) between the parties in the SMART-SIGN™ certificate community or change basic attributes and characteristics or the level of security offered by such certificates.

Non-critical revisions will be versions which:

- add the description of more classes of personal SMART-SIGN™ certificates to the single text without introducing changers to the terms and conditions of previous versions;
- envisage certain additional alternative attributes or characteristics for the services offered by compliant CSPs, without reducing the existing rights of their recipients;
- better clarify some of the procedures mentioned in the previous version of the Policy, without altering the substance of any relationships served by that procedure.

All **critical revisions** will be marked by a change (increase) in the first digit of the version number in the new policy. **Non-critical revisions** will cause the second digit of the version number to change (increase) as compared to the version number of the previous valid policy.

New policy versions as a result of revisions will be assigned **a new unique OID** by ATHEX. Such OID will depend on the **composition** of valid OIDs (detailed in paragraph 1.2.3), the **class** and new **version number** of the resulting policies.

10.2.3 Retroactive effect of revised versions

All revisions of these Policies will **become effective only ten (10) days after their publication** (in accordance with paragraph 10.2.1) and govern all new certificates issued after that data, which **must indicate the new OID** of the policy corresponding to them.

CAs, holders-subscribers and relying parties in respect of SMART-SIGN™ certificates issued based on a valid version of this Policy prior to the revision (namely certificates indicating the OID of a Policy prior to the applicable policy) will still be governed by the terms of that policy, **except for** any non-critical revisions of that policy which in the meantime were published and became effective. **The latter will replace,** as is expressly provided for in this Policy, **previous ones and thereafter govern the relations between the parties involved**.

Approvals of Certification Practice Statements and licenses to claim that other polices are equivalent to or compatible with this Policy on personal SMART-SIGN™ certificates, granted by the Policy Management Committee (in accordance with the following section) **will remain valid and also cover the new versions** of this Policy in the event of **non-critical revisions** (namely versions where the first digit of the version number has not changed, as indicated above). The comparative evaluation of the above texts with new policies on SMART-SIGN™ certificates **which are the result of critical revisions** requires a **new approval** by the Committee for which the following procedures will be repeated.

10.3 COMPARATIVE EVALUATIONS AGAINST THESE POLICIES

10.3.1 Policy Mapping

Where interoperability is required in the applications of personal SMART-SIGN™ certificates with one-way or two-way mapping of these Policies with other policies (issued by another CSP or associated authority) on personal certificates, those other policies which are compared to this Policy must be evaluated by the ATHEX's Policy Management Committee.

In particular as regards **two-way** and mutual policy mapping or **one-way** policy mapping where compatibility or equivalence is attributed to this policy, the aforementioned Committee of ATHEX, being the manager of this Policy, will, after having first performed a suitable legal and technical check on the model being compared with this Policy, **issue a binding decision** regarding ATHEX's Digital Certification Services and any other CSPs who comply with this Policy(who have been approved by it and use this Policy) as to whether there is compatibility and on any required revisions of the texts necessary to achieve compatibility.

In the event of **one-way** policy mapping where compatibility or equivalence is attributed to another policy issued by another CSP or associated Authority who may have applied to the Committee for the attribution of compatibility or equivalence, the Committee may evaluate and approve or suggest any necessary amendments to the text of the policy being compared only after the applicant has paid the specific fees for acquiring the **right to claim equivalence** established by ATHEX's Digital Certification Services.

10.3.2 Approval of compliance of Certification Practice Statements with these Policies

Where a CSP, other than ATHEX's Digital Certification Services, wishes to adopt the terms of these Policies on Personal SMART-SIGN™ *(double key)* – Class 1 certificates of ATHEX as those terms stand, in order to issue to its subscribers certificates entitled Personal SMART-SIGN™ – Class 1 Certificates, including ATHEX's SMART-SIGN™ trademark, that CSP must:

(a) pay to ATHEX such **fees for the joint use of its trademarks** as have been agreed with ATHEX; and

(b) obtain **written approval** from ATHEX's Policy Management Committee on the compliance of that CSP's Certification Practice Statement with this Policy, **also paying any evaluation fees** established by the Committee for the evaluation and final approval procedure.

For a CSP to obtain the above written approval of compliance with this Policy on personal SMART-SIGN™ certificates, the CSP **must submit** its applicable Certification Practice Statement to the Committee in both hard and soft copy **for evaluation by the Committee**, and accept in advance any such necessary amendments to it as the **Committee will instruct at its absolute discretion** to become compatible with this Policy.