Registration Authority Code	01
Registration Authority Ref. No	
Registration Authority Approval Date	
Registration Authority Officer Signature	
Subscriber PIN	

Subscriber PIN			

SUBSCRIBER APPLICATION - AGREEMENT

FOR THE SUPPLY & USE
OF PERSONAL DIGITAL SIGNATURE CERTIFICATES
TYPE SMART-SIGN™ *(double key)* **- 1st CLASS**
(For use in electronic transactions WITHOUT ECONOMIC VALUE)

This **application** serves also as an **agreement** between the applicant and ATHEX SA under the following terms, **only and only when** the competent Registration Authority (RA) of the DCS Network of HELEX **approves** it, after having checked it for completeness and having checked the attached documents and certificates, and the certificates issued to the applicant. This Application - Agreement must be signed by the applicant **IN PERSON** on the last page **before an authorized officer** (Administrator) of a **LSA** of the **DCS NETWORK of ATHEX** or a **PUBLIC AUTHORITY, certifying the authenticity of the signature.**

APPLICANT - SUBSCRIBER INFORMATION

To be completed by the applicant - party

A. INFORMATION OF THE APPLICANT TO BE MENTIONED ON CERTIFICATES

	In **Greek** uppercase characters*	In **Latin** uppercase characters*
FIRST NAME:		
LAST NAME:		
FATHER'S NAME:		
CITIZENSHIP:		

* = As it appears in the attached copy of the applicant's public identification document

E-MAIL ADDRESS:	

(Fill in a valid email address you wish to use to send emails with authentication signature and/or receive encrypted mail. This address shall not be certified by ATHEX but stated in the certificate based on the declaration of the Subscriber, and it shall not change until the expiry of the certificate.)

B. INFORMATION OF THE APPLICANT'S PUBLIC IDENTIFICATION DOCUMENT FURNISHED TOGETHER WITH THE APPLICATION (in legally certified copy)

Type*	Issuing authority	Number	Issued on	Expires on**

* = e.g. Identification Card or Passport   *** = If indicated on the document*

C. MANDATORY CONTACT INFORMATION OF THE APPLICANT - POTENTIAL SUBSCRIBER

Please, use the following information for any contact with me under this Agreement:

ADDRESS:	Street	Number	City/Town	Postal Code	Telephone

COMPANY/ORGANIZATION or PROFESSION:	
FAX:	E-MAIL ADDRESS:
Tax Identification Number:	Tax Office:

D. OPTIONS OF THE APPLICANT - POTENTIAL SUBSCRIBER (Sign in the box of your desired answer)

(a) I do not wish to have my certificates **published** in the *public list* of active certificates of ATHEX (*see Article 7.3*)	**YES** *Signature*	**NO*** *Signature*

* = Default answer if no choice is made by the applicant

LOCAL SUBMISSION AUTHORITY

To be completed and signed by an authorized Administrator of the Local Submission Authority (LSA) of the DCS Network of ATHEX

LSA Name	LSA Protocol No	LSA Protocol Date	Full name of LSA Administrator	Signature of LSA Administrator

TERMS OF THE AGREEMENT

The following terms govern the **Agreement for the supply and use of personal digital signature certificates** made by and between:
(a) the company ATHENS EXCHANGE SA (Reg. No: 34265/01/B/95/512) with its registered offices at 110 Athinon Avenue in Athens (hereinafter **ATHEX**), represented by the LSA authorized to that effect of the the DCS Network of ATHEX indicated on the first page (bottom left); and
(b) the other party (hereinafter **Subscriber**) whose particulars are listed on the first page (application) of this form.

1. Main information and scope of the Agreement

1.1 ATHEX, as the **Certification Service Provider (CSP)** or **Certification Authority**, through the **Public Key Infrastructure (PKI)** it has developed and collaborating third-party companies that make up the **Digital Certification Services Network of ATHEX** (hereinafter **Network**) shall create a "*digital signature creation data*" (digital private encryption keys) which it shall securely transfer to a *secure signature creation device carrier* customized for each subscriber (Smart Card, hereinafter **"special carrier"** or **"carrier"**) and shall also issue, publish and manage personal electronics certificates of the type **Smart-Sign™** (*double key*) -**1st Class** for *digital signature verification data* (public encryption keys) of the subscriber in accordance with the terms and conditions set out in the *Certification Regulation* of **ATHEX** (hereinafter Regulation) and the relevant **Policy on Personal Certifications of the Type Smart-Sign™ (double key) - *1st Class* of ATHEX** (hereinafter the **Certificate Policy** or **Policy**), **as are in force from time to time** and published in the *Digital Repository* (repository) of ATHEX online at http://www.ase.ar/pki/repositore and for which it is agreed that shall be incorporated herein by reference only and form an integral part hereof.
1.2 The subscriber declares that he is aware of the above texts, especially of the terms, conditions and restrictions that they specify. In this context, he shall be entitled to make use of these digital keys, the carrier (e.g. smart card) that activates them and the digital certificates that correspond to them for the entire period of their validity, to **sign digital documents** (whose validity shall be equal to that of handwritten signatures pursuant to Presidential Decree 150/2001) and to **confirm in a valid and binding manner his identity** when connecting and communicating using compatible electronic information systems. The digital signature generated using the "recognized certificate" of the subscriber shall serve always as a handwritten signature and provide full proof of the authenticity of the digital document that bears it before any third party.

2. Application for Approval - Shipment of Carrier, Activation Code & Certificates - Initial Activation - Key Archival

2.1 The entry into force of this Agreement shall not occur without the approval of the subscriber's application by the competent Registration Authority (RA) of the DCS Network of ATHEX and the subsequent issue and shipment of the relevant certificates to the subscriber in accordance with the Regulation. The RA must approve the application **within five (5) working days** of its receipt from the LSA, after having checked the integrity of the applicant subscriber's particulars and supporting documents. Where information is missing from the application or items from the supporting documents submitted, the RA of the DCS Network of ATHEX may either reject the application or request of the subscriber any missing information or documents necessary for the approval in accordance with the Regulation and the relevant Policy of ATHEX, also setting at its discretion a deadline to that end, under penalty to definitely reject the application. **2.2.** If the application is approved, the key pairs created and the certificates issued are stored safely on the customized subscriber-specific **carrier** (smart card), owned by the cooperating *Local Submission Authority* to which this application was submitted or as otherwise specified, which is sent with by special proof of receipt to the subscriber, while the *Activation Code* (PIN) of the carrier is mailed separately in a special envelope; the Activation Code is necessary for using the private keys and certificates contained in the carrier.
2.3 After having been issued by ATHEX, the personal certificates of the subscriber are placed -for security reasons- in **"Suspended Mode"** until the subscriber has requested their initial activation, in accordance with the instructions accompanying the carrier when sent to the subscriber.
2.4 The unreserved acceptance of the carrier (with the private encryption keys and certificates) and the Activation Code (PIN) by the subscriber, **and particularly Initial Activation of the certificates** by him implies the acceptance of the correctness of the information they contain, and full cognizance of the commitment and responsibilities he undertakes by using the digital keys and certificates, as defined herein, the Regulation and the relevant Policy of ATHEX, as well as applicable legislation.

3. Duration/Expiration/Renewal - Revocation/Suspension/Activation - Secret Identification Number - Agreement Termination

3.1 The agreement shall have a duration equal to the duration of the certificates of the type **Smart-Sign™** (double key) - **1st Class** issued to the subscriber, which is **one (1) year** from the issue date and ending on the expiry date of these certificates indicated on them. The obligations of both parties hereunder, under the Regulation and the relevant Policy of ATHEX shall following the expiration or revocation of the certificates, continue to bind the respective parties.
3.2 Renewal of the certificates implies the issuance of new keys and certificates (on a new customized carrier) to the subscriber. ATHEX, **maintaining the initiative to propose the renewal or not of its certificates** to the subscriber (after consultation with the relevant LSA) shall inform the subscriber at least 20 days prior to the expiration of the certificates by sending the relevant renewal application for him to sign.
3.3 In case of violation of the terms of this agreement or the Regulation or the relevant Policy of ATHEX by the subscriber or in any other case provided for in the Regulation and the relevant Policy, ATHEX may revoke or suspend the certificates of the subscriber (done by entering the serial identification number of these certificates in the published **Certificate Revocation List (hereinafter CRL)**), informing the subscriber about it. Also, the revocation or suspension of the specific certificates shall be performed by ATHEX also when the latter is informed by any appropriate means that the subscriber has no longer real, legal and exclusive control of the private keys or their physical carrier.
3.4 Upon expiry or revocation of the certificates of the subscriber, he may not make any use of the carrier and the associated encryption keys and certificates, and must return the carrier to LSA to which it belongs or as otherwise established, if request to do so.
3.5 The revocation or suspension of the certificates can and should be requested by the subscriber himself (for his own protection) in the event of exposure of the keys or the PIN of their carrier to third parties or following loss of their carrier, at which time ATHEX shall, after verifying the origin of the request, must proceed to immediately process it.
3.6 In order **to verify the origin of the request for cancellation** (temporary or permanent) or **activation** of the certificates of the subscribers by the Certificate Revocation Management Authority (CRMA) of the DCS Network of ATHEX, this shall any case be done by telephone or other electronic means provided for (e.g. fax, web form, or e-mail).
3.7 In an emergency certificate revocation situation the procedure is carried out by calling the emergency certificate revocation line at +30 6972999420.

4. Obligations, warranties and limitation of liability of ATHEX - Upper limit of ATHEX liability for 1st Class certificates

4.1 ATHEX must through its Network is responsible vis-a-vis the subscriber: a) for creating suitable "pairs of encryption keys" on a customized subscriber-specific carrier (smart card), observing every procedure prescribed by the Regulation and/or the Policy; b) for issuing, publishing and managing personal certificates of the type **Smart-Sign™** (double key)-**1st Class** for the above Subscriber key pairs (i.e. a "recognized personal certificate" of the type **Smart-Sign™ - 1st Class** and a "**personal authentication certificate**" of the type **Smart-Sign™ - 1st Class**), in compliance with Regulation and relevant Certificate Policies of ATHEX; c) for creating a **"personal identification number" (PIN)** for the subscriber which he shall be indicated in his certificates and which shall be unique to in the environment of the ATHEX Network; d) for revoking certificates when requested by the subscriber and for regularly publishing the updated **Certificate Revocation Lists (CRLs)**, in accordance with the procedures and under the terms of the Regulation and the relevant Policy of ATHEX; e) for publishing in its **"Digital Repository"** and also make available in printed form if requested, the applicable Certification Regulation and Certificate Policies it issues, and any amendments thereto.
4.2 ATHEX shall, vis-a-vis the subscriber and other parties with whom the latter transacts electronically using certificates, guarantee: a) the accuracy of all information contained in the certificate at the time of its initial activation, and the existence of all information required for its issuance in accordance with the provisions of the Regulation and the relevant Policy of ATHEX; b) that the subscriber whose identity is attested in the certificate shall at the time of receipt of the carrier (smart card) have the signature creation data (private key) corresponding to the signature verification data (public key) that can be used additionally; and c) the revocation of certificates shall be published **within 24 hours** of verifying the applicant's identity, **always** in accordance with the terms and following the procedure described in the Regulation and the relevant Policy of ATHEX.
4.3 The above guarantees are provided by ATHEX **only** for use of ATHEX certificates by the subscriber, subject to the limitations and conditions laid down in the relevant Policy of ATHEX.

4.4 ATHEX shall not be liable vis-a-vis any party (subscriber or third party), if it has committed no offense or if its actions were in accordance with the provisions of the Regulation and the relevant Policy of ATHEX. ATHEX shall also not be liable (and thus neither shall be the third parties working 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, problems in network communication and in general in cases of all outside obstacles that may prevent the smooth delivery of services and are not attributed to it.

4.5 ATHEX shall not be liable for any indirect or consequential damages, criminal or disciplinary action or punishment, foregone profits or any other indirect consequences suffered by the subscriber on the occasion of the use of or his reliance on a certain certificate.

4.6 Lastly, ATHEX, unless otherwise provided for herein, in the Regulation or the relevant Policy governing the requested certificates, shall not warrant nor be liable for the appropriateness, quality, lack of error or fitness for a particular purpose of all related services, products and documentation provided or offered by it. The services and products provided to the subscriber by ATHEX and its network shall be provided **"as-is"** and liability for whether they are suitable for the desired purpose or whether they should be used or not shall lie exclusively with the client-subscriber.

5. Obligations and responsibilities of the Subscriber

5.1 The Subscriber must: a) be informed about and know well how to use the signature creation data, digital certificates and their carriers and in generally understand the operation of the public key infrastructures (PKI) before taking any relevant action or using his certificate; b) have read, understood and agreed to all terms and conditions contained in the Regulation and the relevant Certificate Policies of ATHEX; c) provide accurate information in this application for the issuance of certificates and verify the correctness of such information on the certificates **before** requesting their Initial Activation, immediately requesting their revocation in case of errors; d) immediately inform the Registration Authority (RA) of ATHEX or the relevant Local Submission Authority (LSA) about each change in the information declared in this application, and request without delay the **suspension** (pause) or definite **revocation** of his certificates, whenever he suspects or knows that the signature creation data were in any way exposed to third parties; e) to exclusively use, for signature creation, the customized secure signature creation device carrier (smart card) given to him through the LSA in a manner appropriate and consistent with the relevant instructions and not try to export his signature creation data to another carrier; f) change and properly safeguard the activation code (PIN), in accordance with the instructions that came with them and never expose it to any third party; g) protect his private keys and their carrier against damage, loss, disclosure, exposure, alteration or unauthorized or unlawful use; h) refrain, under penalty of indemnifying ATHEX or any other harmed third party, from acts of alteration, modification, unauthorized copying and/or malicious use of the signature creation data, the certificates, the carrier and any software made available by the network of services of ATHEX and the information (catalogs, revocation lists, texts of regulations and policies, etc) ATHEX publishes in its digital repository; **i) not make use of his certificates (1st Class) to process transactions involving any asset of any value,** and he shall be the only one liable for any breach of this term.

5.2 The subscriber declares that he is fully informed and knows everything about his rights and obligations, as well as all possible conditions and hazards involved in electronic communication supported by the certification services of ATHEX. Therefore, he recognizes that any invocation by him of the loss of the carrier, PIN leakage or in general inaccuracy of the certificate shall be void, inadmissible, unfair and contrary to good faith.

5.3 The subscriber shall be exclusively responsible and obliged to repair damage caused to any third parties based on his signature. Particularly he shall be obliged to indemnify ATHEX for any damage suffered directly or indirectly as a result of the breach of his obligations hereunder and under the terms of the Regulation and the relevant Policy of ATHEX governing the use of the requested certificates.

6. Property and rights on products and trademarks

6.1 ATHEX retains all intellectual property rights on databases, the contents of its electronic pages, the electronic certificates it issues, the trademarks and logos, its practices, and all the texts it publishes. The subscriber shall not acquire rights of any kind on the trademarks, service marks, product names, algorithms, techniques, etc. of ATHEX, its suppliers or any third party organization ATHEX works with in providing its services.

6.2 The carrier (smart card) of the generated private keys and certificates of the subscriber is and shall remain the property of the **Local Submission Authority (LSA)** cooperating with the Digital Certification Services Network of ATHEX that assists the subscriber during his registration for the services of ATHEX or as otherwise established and right to use it is granted to him exclusively for the period of validity of the certificate. **The subscriber must return the carrier to the LSA immediately upon its request**. The LSA may request of the subscriber to return the carrier even during the period of validity of the certificates, requesting, however, at the same time their immediate revocation and compensating the subscriber for the subscription paid proportionally to the part that corresponds to the time remaining until the normal expiry of the certificates.

7. Personal Data Processing

7.1 The subscriber shall give to ATHEX and all ATHEX network entities working with ATHEX in providing the services his explicit and unreserved consent to collect, review, process and archive such of his personal data as are necessary for the provision to him of certification services and for his commercial transactions with ATHEX. Such personal data shall be processed in accordance with the provisions of Law 2472/1997 and Law 2774/1999 on the protection of individuals with regard to processing of personal data and such data **shall not be used for any other purpose** without the express consent of the data subject.

7.2 Such personal data shall be collected exclusively from the subscribers themselves during the registration process or the renewed of their subscription and kept (in accordance with paragraph (i) of Annex II of Presidential Decree 150/2001) for 30 years from the expiry of the certificates **to be used in particular to provide evidence in dispute resolution proceedings related to the certification of the digital signatures of the subscriber. The subscriber expressly declares that he is aware of, accepts and agrees to the above processing of his personal data, and that he authorizes ATHEX (or any party succeeding ATHEX in the provision of the relevant services) to disclose to third parties his personal data in any dispute resolution proceedings related to use of his certificates.**

7.3 The subscriber may, at its absolute discretion, which is expressed by his declaration in this application-agreement (which may also be amended later by means of a new written declaration to ATHEX), allow or not the publication of a copy of the his personal certificate (and, therefore, of his personal data listed on it as well) in the shared **list of active certificates** Directory) located in the digital repository of ATHEX for ease of verification of his digital signature by others.

7.4 In any case, the subscriber shall be entitled to appeal to the competent **Registration Authority of the ATHEX Network** (which is in this case his *data controller* according to the law), to make use of his *Information* and *Access* rights under Articles 11 and 12 respectively of Law 2472/1997.

8. Pricing Policy

8.1 The subscriber shall pay to the cooperating LSA of the ATHEX Network such amounts as are set forth herein for registration or renewal subscription fees in respect of the issuance and management of certificates, fees for granting the use of the secure signature creation device carrier (smart card) and any other related costs, and receive from it the relevant tax

documents. Where the ATHEX Registration Authority rejects his application, the subscriber shall be entitled to receive from the LSA a refund of any advance payment made.

8.2 By paying such amounts to the LSA, the subscriber shall fulfill his financial obligations to ATHEX for the issuance, supply and management of the keys and certificates for the entire period of their validity, being entitled to make unlimited use (during such period), in accordance with the terms of the Regulation and the relevant Policy of ATHEX. The "list of active certificates", "certificate suspension, activation or revocation" (by the publication of CRLs) and "certificate verification" digital services (by access to the CRL), as well as access to all the texts published in **digital repository** of ATHEX, shall be **available free of charge** to the subscriber and the third parties concerned on a **24-7-365 basis**.

8.3 With the exception of the cases expressly mentioned herein, the subscriber shall have no other right to refund of the money he paid, especially in cases of revocation of his certificates at his request (due to loss or exposure of the carrier or keys) or their revocation by ATHEX due to the fault of the subscriber.

9. General Terms - Final Provisions

9.1 ATHEX reserves the right to unilaterally amend by its declaration the terms hereof, and to amend the "Certification Regulation" and the relevant "Certificate Policies" it issues in accordance with the procedures and conditions set out in such documents .

9.2 Any manner of declaration, notice or information from ATHEX to the subscriber hereunder or under the Regulation or the relevant Policy shall be deemed to have been validly made if done by e-mail, fax, or mailing to the addresses or calling the contact telephone numbers given by the subscriber in this application-agreement unless the subscriber has informed ATHEX in writing of any change to such information. The subscriber may validly inform or send notices to ATHEX

at the address "ATHEX SA DIGITAL CERTIFICATION SERVICES - 110 Athinon Avenue, 10442 Athens or via telephone at 210 336 6300 or by fax at 210 336 6301 or via email at: PKICA-Services@helex.ar

9.3 Where any provision(s) hereof become(s) (wholly or partly) null and void or unenforceable this shall not render unenforceable all other provisions and this agreement shall be deemed amended in terms of the required deletion or change of the such null and void or unenforceable provision, to become valid, enforceable, and as far as possible, consistent with the original purpose of the parties.

9.4 This agreement shall be governed by Greek law and any dispute in relation hereto shall be brought before the courts of the city of Athens, to the exclusive jurisdiction of which the parties shall hereby be subject.

PLEASE READ CAREFULLY AND SIGN BEFORE A CERTIFYING PUBLIC AUTHORITY OR AUTHORIZED LSA OF THE DCS NETWORK OF ATHEX

By signing this application-agreement I hereby **expressly declare** and **accept** that:

1) my particulars indicated in this application are **correct** and **I agree that they be processed** by ATHEX,
any lawful successor of ATHEX and agencies collaborating with it for the provision of Digital Certification Services, in accordance with the terms hereof (and in particular Article 7);

2) I have carefully read the above terms and **I unreservedly accept all of them** and **declare that I have received** –in a language I can understand- a copy of the **"Summary Notice of ATHEX Certification Services"** with a summary of the terms, conditions and information contained in the **"Certification Regulation"** of ATHEX and the **"Policies of Personal Certificates of the type Smart-SignTM"** of ATHEX governing the use of the carrier (smart card) of my private keys and certificates.

Date: ..../........../ 20.......

The Applicant and Declarant

....

Certification of signature authenticity here

Note: Attached hereto is submitted <u>a duly certified copy of a public document of identification</u> (e.g. passport or identity card) used to prove the accuracy of the applicant's personal data given in this application.

Note: Attached hereto I submit legally certified true copies of my identity card or passport, which serve to prove the accuracy of my personal information given in this application for certification by ATHEX.