Hellenic Public Administration Root Certification Authority

(HPARCA)

SERVICE AGREEMENT FOR THE PROVISION OF ELECTRONIC IDENTIFICATION SERVICES TO SUBSCRIBERS

General Terms and Conditions of Use of Electronic Identification

Version 1.0

Publication history

Date	Version	Changes
30/6/2026	1.0	Original document

Acronyms and Definitions

Definitions

Table 1: Table of Definitions

Mount	Definition
Registration Authority (RA)	An entity that has been approved by the HPARCA or another CA and assists the interested parties for electronic identification means during the submission of their applications, approves or rejects the registrations / applications as well as requests the Certification Authority to revoke electronic identification means.
Certification Authority (CA)	An entity that is certified to issue, handle and revoke electronic identification means.
Relying Party	A natural or legal person who relies on electronic identification.
Public Key	The part of key pair that can be made public by the owner of the respective private key and which is used by a Relied Party to verify an approved certificate created with the corresponding private key of the owner and/or to encrypt messages so that they can only be decrypted with the corresponding private key of the holder.
Identification data	A data set that allows the identification of a natural or legal person or a natural person representing other natural or legal persons.
Qualified Signature Creation Device	Electronic signature creation device that meets the requirements of Annex II of Regulation (EU) 910/2014 (eIDAS) and is under the exclusive control of the user.
Remote Qualified Signature Creation Device	An approved e-signature creation device, managed by an approved trust service provider on behalf of a signatory, in accordance with Article 29a of the eIDAS Regulation.
Qualified Trust Service Provider	A trust service provider that provides one or more approved trust services and has been recognised as such by the Supervisory Body. In this case, HPARCA.
Exposure to Risk	The violation of a security policy, during which unauthorized access/disclosure may have occurred, or loss of control over the information collected for the provision of the approved trust services of the HPARCA. As far as private keys are concerned, exposure to risk is the loss, theft, disclosure, unauthorized use of this private key.
Confidential Information	The information necessary to remain confidential and personal.
Identity Verification	An electronic process that allows the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form.

Level of assurance	The degree of trust in the identity invoked or declared by a person and designated in accordance with the relevant technical specifications, standards and procedures, including the technical controls governing the relevant electronic identification means, issued in the context of an electronic identification system. It is divided into low, basic and high as provided for in Commission Implementing Regulation (EU) 2015/1502.
Register or Apply	The electronic procedure described in the HPARCA Certification Regulation and which concerns the steps that the Subscriber must take in order to acquire means of electronic identification.
Private Key	The key of a key pair that is kept hidden from the owner of the key pair and that is used to create qualified certificates or to decrypt electronic files or folders that have been encrypted with the corresponding public key.
List of Revoked Certificates (CAS)	The periodic (or extraordinary) list issued electronically and signed by a CA, of the Certificates that have been revoked before their expiration date. The CAP states the name of the issuer of the CAP, the date of issue, the date of the next scheduled issuance of the CAP, the serial numbers of the revoked Certificates, as well as the specific times and reasons for their revocation.
Authentication Certificate	An electronic certificate that is used to electronically identify a natural person and confirms their identity.
Certificate Policy (CP)	Named set of rules indicating the applicability of a certificate to a specific community and/or application category with common security requirements.
Primary Certification Authority (Root CA)	A CA that acts as a Primary CA (Root) and issues certificates to underlying CAs. In the current infrastructure, HPARCA operates as a Primary Certification Authority.
Subscriber (End User)	The person who is the Subject, in whose name a Certificate has been issued. The Subscriber (End User), or the applicant for the certificate, is authorized to use the private key corresponding to the public key indicated on the Certificate and is responsible for the proper use of the certificate in accordance with the Certificate Terms and Conditions of Use (TOS).
Electronic Identification Scheme	An electronic identification system under which electronic identification means are issued to natural or legal persons, or to natural persons representing other natural persons or legal persons.
Public Key Infrastructure (PKI)	The architecture, organizational structure, techniques, regulations, and procedures that together support the implementation and operation of a Certificate-based public key cryptographic system
Underlying Certification Authority (eID)	The issuing certifying authority responsible for the issuance, revocation and general lifecycle of subscriber authentication certificates.
Subject	The owner of a private key that corresponds to a public key. The authenticated name of a Certificate Subject is linked to the public key included in the Certificate.
Storage or Repository	The network-accessible database of the Certification Authority of the Greek State which contains the details of the Certificates as well as other information related to the Public Key Infrastructure of the Certification Authority of the Greek State (HPARCA).
eIDAS Regulation	Regulation (EU) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 'on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC', as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 'amending

	Regulation (EU) No 910/2014 of the European Parliament and of the Council 910/2014 establishing a European Digital Identity Framework"
OCSP (Online Certificate Status Protocol)	The protocol used to provide Based Parties with real-time information about the status of Certificates.

Acronyms

Table 2: Table of Acronyms

Acronym	Oros (in Greek and English)
(English)	
eIDAS	eIDAS Regulation
ETSI	European Telecommunications Standards Institute
OCSP	Online Certificate Status Protocol (Πρωτόκολλο Δικτυακής Κατάστασης Πιστοποιητικών)
PIN	Personal identification Number
RA	Registration Authority
CA	Certification Authority
HPARCA	Certification Authority of the Greek State
QSCD	Approved Signature Creation Device
EETT	National Telecommunications and Post Commission
QTSP	Approved Trust Service Provider
CRL	Certificate Revocation List
QSCD	Cryptographic Signature Module
CPS	Certification Practice Statement
OID	Object Identifier
RCA	Root Certification Authority
eIDP	Electronic Identification Provider
CP	Certificate Policy
TSP	Trust Service Provider
PKI	Public Key Infrastructure
	Underlying Certification Authority
LoA	Level of Assurance
OTP	One-time Password

1. General Terms

These General Terms and Conditions (hereinafter "Terms and Conditions") describe the main policies and practices followed by the Hellenic Public Administration Root Certification Authority (HPARCA) and are provided for in the Regulation of Electronic Identification of HPARCA, which is posted on the electronic repository of HPARCA (https://pki.aped.gov.gr/repository) and define the obligations and rights of HPARCA and the Subscribers (End Users) during the provision of electronic identification services by HPARCA, in the framework of the Greek electronic identification scheme (eID scheme). The purpose of the scheme is the reliable electronic identification and authentication of users when accessing public and

private electronic services, with a level of assurance determined in accordance with the applicable EU and national regulatory framework.

Within the framework of the scheme, HPARCA issues and manages the certificates that support the operation of electronic identification means. These certificates for electronic identification (hereinafter referred to as 'certificates' or 'electronic identification certificates') are electronic certificates, which identify the holder of the certificate.

1.1 The Terms and Conditions govern the use of electronic identification means by the Subscribers (End Users) and constitute a legally binding contract between the Subscriber and HPARCA.

1.2 The Subscriber must be aware of and accept these Terms and Conditions.

1.3 HPARCA has the right to amend the Terms and Conditions at any time if there is a justified need for such amendments. The current version as well as all previous ones are published on https://pki.aped.gov.gr/repository website.

1.4 Subscribers (End Users) means natural persons, holders of electronic identification means who have legal capacity, are Greek citizens, over twelve (12) years of age. Each citizen has only one means of electronic identification regardless of the level of assurance.

1.5 The means of electronic identification of a natural person can be issued only if the identification of the natural person to whom they are to be issued has been successfully carried out. Acceptable identification documents are defined in the Electronic Identification Regulation of the HPARCA.

2. Identification, Application and Acceptance of electronic identification means

2.1 Upon registration, the applicant must submit to the HPARCA the relevant application, as well as the necessary identification documents, as indicated by the HPARCA. The applicant must submit accurate, true and complete information. By submitting an application for the issuance of electronic identification means, the applicant confirms that he/she is aware of and accepts the Terms and Conditions.

2.2 **Identification.** The electronic identification means issued under the scheme are classified at the assurance level of LoA Substantial and High.

- For the High Assurance Level, identity verification (identification) is carried out by prior verification of all Subscriber Identification Data only with physical presence.
- For the Substantial Assurance Level, identity verification is carried out by prior verification of all the Subscriber's Identification Data either a) by physical presence, or b) by using remote authentication methods that satisfies the substantial level of assurance in accordance with the requirements of Implementing Regulation (EU) 2015/1502.

Identification, which is carried out either through the physical presence of the person (applicant) or remotely, requires the presentation of an acceptable identification document to an authorized employee

of the RA or the delegated, Local RA (LRA) Office of the HPARCA. In the case of fully automated remote identification, it is required to show an eligible identification document in the application/software. The HPARCA may delegate part or all of the identification process to a third party.

2.3 **Acceptance of Certificate**. The following actions constitute acceptance of the Certificate:

- The issuance of the Certificate constitutes the acceptance of the Certificate by the Subscriber
- Failure to object to the Certificate or its contents within 24 hours of its receipt constitutes acceptance of the Certificate.

For the purposes of this section (2.3), the term Certificate includes the case of other means of electronic identification, as issued at the Substantial assurance level.

2.4 **Means of Electronic Identification, Use and Applicable Policy**

Means of electronic identification	**Level of assurance**	**Applicable and Published Certification Policy**	**Duration by definition**
Certificate of authentication/electronic identification issued to a remote QSCD	High	Regulation of Electronic Identification of HPARCA published at https://pki.aped.gov.gr/repository ETSI Policy EN 319 411-1: NCP+	3 years since their issuance
The Identification Data and cryptographic identifier of the paired device as stored in the Electronic Identification Provider (IdP) Database/LDAP	Substantial	Regulation of Electronic Identification of HPARCA published at https://pki.aped.gov.gr/repository	3 years since their issuance

3. Duration/Expiration/Renewal – Revocation/Suspension/Activation – Termination of Contract

3.1. The contract has a duration equal to the validity period of the electronic identification means issued to the Subscriber, which is three (3) years from their issuance and expires on the "expiry date" of the above certificates, which is stated therein. The obligations of both parties provided for by these Terms and Conditions and the relevant Electronic Identification Regulation of HPARCA for after the expiration or revocation of the electronic identification means, continue to be borne by the liable parties.

3.2. The renewal of the electronic identification certificate does not apply but consists of the regeneration of certificate keys. Certificate key regeneration is the revocation of the old certificate and the application

for the issuance of a new electronic identification certificate that corresponds to the new public key. Keys for the certificate can be regenerated after it expires.

3.3. In case of violation of the terms hereof or of the HPARCA Electronic Identification Regulation by the Subscriber, or in any other case provided for in the Electronic Identification Regulation, HPARCA may revoke or suspend the electronic identification means of the Subscriber by informing the Subscriber accordingly. Also, the revocation or suspension of the affected means of electronic identification is carried out by the HPARCA in the event that the latter is informed, in any appropriate way, that the Subscriber no longer has real, legal and exclusive control of his/her private keys.

3.4. The revocation or suspension of the means of electronic identification may, but is also mandatory, be requested by the Subscriber themselves (for their protection) in case of exposure of his keys or PIN to third parties, or after the loss of the paired mobile device, in which case the HPARCA must, after verifying the origin of the request, proceed to its immediate processing.

3.5 In the case of an electronic identification certificate, the revocation is carried out by adding the certificate identification serial number to the published Certificate Revocation List (CRL), and also by the corresponding response of the OCSP server.

4. Prohibitions on Use

4.1 The electronic identification means are not designed, intended or approved to be used in situations where highly classified data or highly security conditions are required (such as national defense and security).

4.2 The electronic identification means of the Subscriber are prohibited from being used outside the limits and content specified in the Electronic Identification Regulation of HPARCA or for illegal purposes, or contrary to the public interest, or otherwise for a purpose that may harm the Greek State and/or HPARCA. Indicatively, the use of electronic identification means is prohibited for any of the following purposes:

4.2.1 illegal activity (including cyber-attacks and attempted breach of the Certificate)

4.2.2 Facilitating other parties to use the means of electronic identification, except in the case of legal representation, as defined by Article 24A of Law 4727/2020, as in force

4.2.3 Facilitating automated use of electronic identification means

5. Trust Limits

5.1 Trust Limits for Electronic Identification Means

5.1.1 The information associated with electronic identification means shall be accurate. There shall be no errors or misrepresentations in respect of this information, known to or emanating from the entities authorising the extradition request or issuing these instruments.

5.1.2 The means of electronic identification are valid from the date of issue as specified in the relevant Catalogue (LDAP). The validity of the means expires upon their revocation or otherwise on the expiry date indicated in the Catalogue, which is 3 years from the date of issue. In addition, in the case of an electronic identification certificate, the period of validity is also indicated on the dates of commencement and expiry of the certificate. In case of revocation of the certificate, the revocation date is indicated in the CRL and in the OCSP server's response.

5.1.3 The audit records are kept within the system for at least two (2) months. Physical or digital records relating to Certificate applications, registration information and requests or requests for suspension, termination of suspension and revocation shall be retained for seven (7) years after the expiration of the relevant Certificate.

6. Rights and Obligations of the Subscriber

6.1 The Subscriber has the right to submit an application for the issuance of electronic identification means, by accepting these Terms and Conditions and complying with the requirements of the Electronic Identification Regulation of HPARCA.

The Subscriber must proceed with the issuance of the means of electronic identification within thirty (30) days from the identification to the Authorized Office. After this period, their application is cancelled and they must submit a new application.

6.2 The Subscriber:

a) Shall submit accurate, true and complete information regarding the issuance of the means of electronic identification and inform the HPARCA of the correct information within a reasonable period of time, in case of change of his/her personal data or of any inaccuracies of the information related to the means of electronic identification.
b) Shall submit the necessary documents and supporting documents for their identification to the HPARCA as specified in the application form for the issuance of electronic identification means, as well as follow the steps indicated by the HPARCA to complete the registration process
c) Shall not proceed with the procedure for issuing electronic identification means, if they do not have the legal right to do so, and/or do not have legal capacity or the required age.
d) Is solely and fully responsible for any consequences of the use of their electronic identification means both during and after their expiry.
e) Is solely responsible for any damage caused due to inability or unlawful fulfillment of their obligations set forth in the Terms and Conditions and/or the Greek and European Union laws.

6.3 **Security measures**.

The Subscriber:

a) is solely responsible for the secrecy of private keys and their access authentication factors (PINs);
b) is responsible for maintaining adequate security and control over all credentials, passwords, PINs or any other codes used to access the appropriate application from the official application repository of the mobile device's operating system;
c) must ensure that the Subscriber's Private Key is used under their control and exercise due diligence to avoid its unauthorized use;
d) is responsible for the correct and safe use of the mobile device used during the application process for Electronic Identification or, in particular, the supply and installation of the appropriate application,
e) if the Subscriber's device is lost or destroyed or the Subscriber is unable to use the means of electronic identification for any reason outside the control of the HPARCA, the Subscriber must immediately contact the HPARCA to request the revocation of the means of electronic identification,
f) must immediately inform the HPARCA of the possibility of unauthorized use of their Private Key or if their Private Key has been lost, stolen, possibly compromised or if control of their Private Key has been lost due to compromise of authentication credentials or for other reasons and immediately revoke his/her means of electronic identification; and
g) must not continue to use the private key if its means of electronic identification have been revoked or if the IP has been compromised.

6.4 The Subscriber declares that they have been fully informed and is aware of everything regarding their rights and obligations, as well as all possible conditions and risks of electronic communication supported by the electronic identification services provided by HPARCA. It therefore acknowledges that their allegation of loss of connection, leakage of the PIN or inaccuracy of the relevant information in general is invalid, inadmissible, abusive and contrary to good faith.

6.5 The Subscriber accepts that, during the process of issuing, revoking and generally managing their certificate, they will receive informative SMS/email.

6.6 The Subscriber shall not assign their rights or transfer the obligations to third parties under these Terms and Conditions. Any attempt to delegate or authorize, except in the case of legal representation, as defined by Article 24A of Law 4727/2020, as in force, will be considered invalid.

7. Obligations of HPARCA

Without prejudice to section 9, HPARCA is obliged to provide the services in accordance with the Electronic Identification Regulation.

7.1 HPARCA shall, towards the Subscriber:

a) provide the electronic identification services in accordance with the applicable agreements set out in paragraph 9 and the relevant legislation;
b) create a pair of cryptographic keys in compliance with all the procedures provided by the Policy;

c) issue and manage the means of electronic identification in accordance with the provisions of the relevant Electronic Identification Regulation of the HPARCA,
d) revoke the Subscriber's means of electronic identification when requested and, in the case of certificates, to publish the Certificate Revocation List at regular intervals, as well as for the OCSP server to respond to the status of the certificate, in accordance with the provisions of the relevant Electronic Identification Regulation of HPARCA,
e) publish and inform the Subscribers in any appropriate way or means, about the policies and in general binding documents issued by the Subscriber, as well as any modification thereof;

7.2 HPARCA guarantees to the Subscriber:
a) the accuracy of all information related to the means of electronic identification and the existence of all the data required for its issuance, in accordance with the relevant Policy of the HPARCA,
b) that the revocations of electronic identification means will be activated/published within 24 hours from the submission of the relevant application, always in accordance with the terms and procedure described in the HPARCA Certification Regulation.

7.3 The HPARCA complies with the provisions of the eIDAS Regulation.

7.4 The above guarantees are provided by HPARCA only for the use of the means of electronic identification issued by the Subscriber.

7.5 HPARCA shall not be liable to anyone (subscriber or third party) if they are guilty of a fault or if their actions were not in accordance with the provisions of these Terms and Conditions. HPARCA is also not responsible for any malfunction of its services in cases of force majeure, such as earthquakes, floods, fires, etc., including cases of black-out, problems in telecommunications networks and in general all external obstacles that may hinder the smooth provision of its services and are not due to its fault.

8. Obligations of Conditional Review by Relied Parties

8.1 Each Relying Party shall consider the risks and responsibilities associated with the acceptance of electronic identification means. The risks and responsibilities have been defined in the CP. A Relying Party acknowledges that it has access to sufficient information to ensure that it is able to make an informed decision on the level of assurance required and the extent to which it chooses to rely on the associated information of the electronic identification means.

8.2 Each Relying Party accepts and agrees that the use of the HPARCA Repository and its reliance on any Certificate is governed by the applicable Electronic Identification Regulation of HPARCA which is published in the Repository at: https://pki.aped.gov.gr/repository. Amendments thereto are also published at the same address.

8.3 The obligations of the Relied Party have been defined in the Electronic Identification Regulation of the HPARCA.

8.3.1 Electronic identification means shall be used only to the extent that their use is in accordance with applicable legislation and permitted use under the Electronic Identification Regulation and these Terms and Conditions. The electronic identification means of the HPARCA are not designed, intended to, or approved for use or resale as control equipment in hazardous conditions or for uses that require the safe operation versus error, such as in the operation of nuclear installations, aircraft navigation or communication systems, air traffic control systems or weapons control systems, where an error could directly lead to death, personal injury or significant environmental damage.

8.4 The HPARCA ensures that the electronic identification infrastructure is available on a 24-hour basis, 7 days a week, with a minimum total availability of 99% per year with planned outages not exceeding 0.4% per year.

8.5 In the case of certificates, if sufficient validity information is not contained in the Certificate, the Relied Party may verify the validity of the Certificate by checking the OCSP and CRL reports found in the Certificate.

9. Limited Warranty and Disclaimer/Limitation of Liability

9.1 HPARCA is responsible for issuing the means of electronic identification as defined by the Law and the CP of HPARCA.

9.2 HPARCA informs all Subscribers and Subjects before terminating the electronic identification service and maintains the documentation regarding the interrupted service as well as the information required in accordance with the procedure set out in the CP.

9.3 HPARCA is not responsible for:

a) the confidentiality of the credentials of Private Keys located in a remote QSCD, for loss or destruction of the mobile device used as an authentication factor,

b) any improper or permissible use of electronic identification means or inadequate checks thereof or for the erroneous decisions of a Relying Party or any consequences due to error or omission of their power check;

c) for the non-fulfilment of its obligations if such non-fulfilment is due to errors or security problems of the supervisory body, the Trust List or other public authority;

d) for the inauthenticity of the identification documents used for electronic identification, nor for any damage that may be caused to the Subscriber or to third parties due to this cause, provided that he/she has duly followed the prescribed identification procedures, and

e) for non-fulfillment if it is due to force majeure.

9.4 HPARCA provides limited warranties and disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability and excludes all liability, other than willful misconduct or gross negligence, for any loss of profits, loss of data, or other indirect, incidental, or punitive damages arising out of or in connection with the use, delivery, license, performance, non-fulfillment or unavailability of certificates, electronic identification means or any other transactions or services provided or referred to herein, even if HPARCA has been informed of the possibility of such damages.

The Greek State is liable for damage caused by acts or omissions of the HPARCA bodies or the issuing CAs to any natural or legal person, due to non-compliance with the obligations provided for in the Code of Civil Procedure, in accordance with article 105 of the Introductory Law of the Civil Code (Introductory Law). Limitations of liability include the exclusion of indirect, special, consequential, and consequential damages. In particular, for the liability of the Greek State due to acts or omissions of the bodies of the HPARCA, in terms of compliance with the provisions hereof, the following apply:

The Greek State is not responsible for any malfunction of the services of HPARCA in cases of force majeure, such as earthquakes, floods, fires, etc., including cases of black-out, problems in the telecommunications networks and in general all external obstacles that may hinder the smooth provision of its services and are not due to its fault.

In addition, the provisions of paragraph 2 of Article 13 "Liability and burden of proof" of Regulation 910/2014 apply and apply in this case, pursuant to par. 3 of the same article.

9.5 Subscribers, Subjects and Relied Parties are hereby informed of the possibility of theft or other form of compromise of a private key corresponding to a public key included in a certificate or otherwise used as a means of electronic identification, which may or may not be traceable, as well as of the possibility of the use of a stolen or compromised key.

9.6 HPARCA may terminate the identification process if any information provided by the Subscriber during the identification process is inaccurate or untrue or there is a suspicion that the Subscriber has provided inaccurate or untrue information or the verification of the Subscriber's identity is not successful.

10. Applicable Policies & Statements of Certification Practices

Relevant certificate policies and declarations of practices related to these Terms and Conditions can be found in the Electronic Identification Regulation of HPARCA

The current version of the above document is published at: https://pki.aped.gov.gr/repository

11. Privacy and Confidentiality Policy

11.1 HPARCA adheres to the Privacy Policy on Electronic Identification, which is included in the HPARCA Repository at the address (https://pki.aped.gov.gr/repository) and the legislation of the European Union, when processing personal data during the provision of electronic identification services.

11.2 All information that has become known during the provision of services and is not intended for disclosure (e.g. information that was known to HPARCA) is confidential. The Subscriber has the right to receive information from HPARCA regarding the personal data processed by HPARCA, in accordance with the General Data Protection Regulation (EU Regulation 2016/679) and Greek legislation.

11.3 HPARCA protects confidential information as well as information intended for internal use so that it is not exposed to risk and does not disclose it to unauthorized third parties.

11.4 HPARCA has the right to disclose information about the Subscriber to third parties, who, according to the relevant legislation, are entitled to receive such information.

11.5 In addition, non-individualized statistics on HPARCA services are also considered public information. HPARCA may publish non-personalized statistics on its services.

12. Refund Policy

HPARCA provides electronic identification services in accordance with the billing policy.

For the needs of penetration of electronic identification and/or replacement of existing passwords in the Single Digital Portal, HPARCA is committed to providing the first 100,000 means of electronic identification at no cost (free of charge).

13. Applicable law, complaints and dispute resolution

13.1 Disputes between the HPARCA, the issuing CAs, the Subscribers and the Relying Parties shall be resolved in accordance with the applicable laws governing the relationship between the parties.

13.2 To the extent permitted by law, prior to recourse to any dispute resolution mechanism in relation to a dispute relating to any aspect of HPARCA's trust services, the Subscriber or any other party to the dispute must notify HPARCA and any other party involved in the dispute regarding any claim or complaint, no later than thirty (30) calendar days from the establishment of the basis of the claim; unless otherwise provided by law. If the dispute is not resolved within sixty (60) days after the initial notice, then the party may resort to litigation. All parties agree that the courts of Athens, Greece, have exclusive jurisdiction and are competent to resolve any dispute relating to the interpretation and execution of these terms and the provision of HPARCA services.

13.3 All requests regarding disputes should be sent to the contact details included in these Terms and Conditions.

14. Storage Permissions, Reliability Marks and Audits

The HPARCA is assessed in accordance with EU Regulation 910/2014 (eIDAS) by an independent conformity assessment body at regular intervals or whenever there is a significant change in the functions of the Electronic Identification Service.

In addition to compliance checks, HPARCA is entitled to carry out other inspections to ensure the reliability of its services.

HPARCA is entitled to carry out a second round of audits on contractors who have entered into a relationship with HPARCA in order to operate as Authorized Offices.

15. Contact Details

The contact details for the Certification Authority of the Greek State are published on the website: www.aped.gov.gr

16. Validity of Terms and Conditions

16.1 The validity of this text of Terms and Conditions begins with the publication of the Electronic Identification Regulation of HPARCA in the Government Gazette. This text is then published immediately in the HPARCA web repository.

16.2 This text of the Terms and Conditions will remain in force until it is replaced by any new, amended version. Amended or new versions are published in the HPARCA repository.

16.3 If any provision of these Terms and Conditions, or its enforceability, becomes for any reason and to any extent invalid or unenforceable, then the finding of invalidity or unenforceability shall not affect the remainder thereof (and the application of the invalid or unenforceable provision to other persons or circumstances), and shall be construed in a manner that reasonably fulfils the purpose of the parties.