Hellenic Public Administration Certification Authority (APED)

CONTRACT FOR THE PROVISION OF TRUSTED SERVICES OF APED WITH A SUBSCRIBER

GENERAL TERMS AND CONDITIONS OF USAGE FOR QUALIFIED TRUST SERVICES

(Qualified Electronic Signatures and Timestamps)

Version 1.1

Version History

Date	Version	Changes
15/12/2021	1.0	Initial Document
13/10/2022	1.1	Translation in English

Definitions and Acronyms

Definitions

Table 1: Definitions Table

Term	Definition
Administrator	A Trusted Person within the organization that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Advanced electronic signature	An electronic signature that meets the following requirements • it is uniquely linked to the signatory; • it is capable of identifying the signatory; • it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and • it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
Certificate	Public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it
Certificate Applicant	An individual that requests the issuance of a Certificate by a CA.
Certificate Application	A request from an Applicant to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing a Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Policy (CP)	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that have been revoked by the certificate issuer
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued
Certification Authority (CA)	An entity authorized to create and assign certificates
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
Compliance Audit	A periodic audit that a TSP, Processing Center, Service Center or Managed PKI Customer undergoes to determine its conformance with legislation, policies and standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss,

	theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/ Personal Information	Information that is necessary to remain confidential and personal.
Coordinated Universal Time (UTC)	Second-based time scale as defined in Recommendation ITU-R TF.460-5
eIDAS	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.
Electronic Document	Any content stored in electronic form and in particular as text or with an audio, visual or audio-visual recording
Electronic Signature	Data in electronic form which are attached to or logically associated with other electronic data and which is used by the signatory to sign.
General Terms and Conditions for Use of Qualified Trust Services	A binding document setting forth the terms and conditions under which a natural or legal person acts as a Subscriber or as a Relying Party and ADACOM provides the corresponding Trust Services.
Hardware Security Module (HSM)	The Electronic Signature Product used by Qualified Trust Service Providers that is protected against modification and ensures technical and cryptographic security (A hardware unit that stores cryptographic keys to keep them private while ensuring they are available to those authorized to use them).
Intellectual Property Rights	Rights in one or more of the following: any kind of copyright, trade secret, trademark, and any other intellectual property right
Issuing Certification Authority	In relation to a particular Certificate, the Certification Authority (CA) that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a Qualified Certificate may provide proof in support of a determination of non-repudiation by a tribunal, but does not by itself constitute non-repudiation.
OCSP (Online Certificate Status Protocol)	A protocol for providing Relying Parties with real-time Certificate status information.
Online Registration or Application	The electronic process described in the Certification Regulations of the Issuing CAs and which concerns the steps the Subscriber must take in order to obtain a digital certificate
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS # 10	Public-Key Cryptography Standard #10 developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS # 12	Public-Key Cryptography Standard #12 developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Precise Time	Reference of data with which year, month, date, time, minutes and seconds are determined. Exact time for Public Sector Bodies is determined based on

	the National Time of Greece.
Private key	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create a qualified certificate or to decrypt electronic records or files that were encrypted with the corresponding public key
Primary Certification Authority (PCA)	A CA that acts as a root CA and issues Certificates to CAs subordinate to it.
Processing Center	The site that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates.
Public Key	The key of a key pair that may be publicly disclosed by the holder of corresponding private key and that is used by Relying Party to verify a qualified certificate created with the holder's corresponding private key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding private key.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The DigiCert PKI consists of systems that collaborate to provide and implement the DigiCert PKI.
Qualified Certificate	Qualified Certificate is a Certificate issued by a CA which has been accredited and supervised by authorities designated by an EU member state and meets the requirements of eIDAS.
Qualified Certificate for Electronic Signature	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation.
Qualified electronic Signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and is based on a qualified certificate for electronic signatures
Qualified signature creation device (QSCD)	A device that is responsible for qualifying digital signatures by using specific hardware and software that ensures that the signatory only has control of their private key. Qualified electronic signature or seal creation devices meet the requirements of eIDAS.
Qualified Timestamping Service Provider	The entity that issues timestamping in accordance with the EETT accreditation framework and is included in the EETT Trusted List of Qualified Trust Service Providers (TSL)
Qualified Trust Service Provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body.
Registration Authority (RA)	An entity approved by a CA that is responsible for identification and authentication of subjects of certificates. Additionally, a RA can assist in the certificate application process or revocation process or both.
Relying Party	An individual or organization that acts in reliance on a certificate.
Remote Qualified Signature Creation Device (Remote QSCD)	Qualified Remote Signature Creation Device that meets the requirements of Annex II of the eIDAS Regulation
Repository of APED	The web-accessible database of the Hellenic Public Administration Certification Authority (APED) which contains the details of the Certificates as well as other information related to the Public Key Infrastructure of APED.
Root CA	Certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s).
RSA	A public key cryptographic system invented by Rivest, Shamir and Adelman.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications

	developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/ Internet Protocol connection.
Subordinate CA (Sub CA)	Certification authority whose Certificate is signed by the Root CA, or another Subordinate CA. A subordinate CA normally either issues end user certificates or other subordinate CA certificates.
Subject	The holder of a private key corresponding to a public key.
Subscriber	An entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations.
Supervisory Body	The authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state.
Timestamp Service	The creation of the necessary evidence for a set of data in digital form, so that it can be proven that this data existed at a certain point in time
Timestamp Token (TST)	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Timestamping Authority (TSA)	The Authority of the Timestamping Services which issues Timestamp Tokens.
Timestamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single Timestamp Token signing key active at a time.
Trust Service	Electronic service for: • creation, verification, and validation of digital signatures and related certificates; • creation, verification, and validation of timestamps and related certificates; • registered delivery and related certificates; • creation, verification and validation of certificates for website authentication; or • preservation of digital signatures or certificates related to those services.
Trust Service Provider	An entity that provides one or more Trust Services.
Trusted Person	An employee, contractor, or consultant of an entity, responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.

Acronyms

Table 2: Table of Acronyms

Term	Definition
APED	Hellenic Public Administration Certification Authority
CA	Certification Authority
CC	Common Criteria
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request

EETT	Hellenic Telecommunications & Post Commission
ELA	Evaluation Assurance Level.
LRA	Local Registration Authority
LSVA	Logical Security Vulnerability Assessment
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PCA	Primary Certification Authority
PDS	PKI Disclosure Statement
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
QSCD	Qualified Electronic Signature Creation Device
RA	Registration Authority.
RCA	Root Certification Authority
RFC	Request For Comment
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
SubCA	Subordinate Certification Authority
TP	Timestamping Policy
TPS	Timestamping Practice Statement
TSA	Timestamping Authority
TSP	Trust Service Provider
TST	Timestamp Token
TSU	Timestamping Unit

1. General Terms

The present General Terms and Conditions describe basic policies and practices followed by the Hellenic Public Administration Certification Authority (APED) and provided for in the following documents:

- Certificate Policy and Practice Statement for Qualified Electronic Signatures of APED, as defined in the Certification Regulation of the Hellenic Public Administration Certification Authority
- Certificate Policy and Practice Statement Timestamp Authority of APED, as defined in the Certification Regulation of the Hellenic Public Administration Certification Authority

while described in complementary manner and in summary in the

- PKI Disclosure Statement (PDS) of APED for Qualified Electronic Signatures and
- Timestamp Disclosure Statement of APED.

1.1. The present Terms and Conditions govern the use of Qualified Certificates for Electronic Signatures and Time Stamps by the Subscriber and constitute a legally binding agreement between the Subscriber and APED.

1.2. Subscriber shall be familiar with and accept the present Terms and Conditions

1.3. APED reserves the right to amend the Terms and Conditions at any time and without notice, if there is a justified need for such amendment. The current version and previous versions are published on https://pki.aped.gov.gr/repository

1.4. The subscriber can submit an application for a Qualified Electronic Signature (stored in QCSD) for a natural person. Identification is carried out through the physical presence of the person (Subscriber) who submits the identification document specified in the Application for the issuance of a Qualified Certificate of Electronic Signature to an authorized employee of the RA or the APED LRA (Authorized Office)

1.5. The invalidity or unenforceability of any provision or provisions hereof (in whole or in part) shall not render all other provisions unenforceable and this shall be deemed amended to the extent necessary to delete or modify the invalid or unenforceable provision so as to become valid, enforceable, and to the extent possible, consistent with the original intent of the contracting parties.

2. Acceptance of Qualified Certificate of Electronic Signature

2.1. By submitting an application for the issuance of a Qualified Certificate for Electronic Signature, the Subscriber confirms that he/she knows and accepts the Terms and Conditions
The following actions constitute acceptance of the Qualified Certificate of Electronic Signature:

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

2.2. If a Certificate key is reissued, the Subscriber confirms that he/she has read and agrees with the Terms and Conditions

2.3. Certificate Type, Usage and Applicable Policy

Certificate Type	**Usage**	**Applicable and Published Certification Policy**
Qualified Electronic Signature that complies with the eIDAS regulation.	Data in electronic form which is attached to other electronic data or logically associated with other data in electronic form and which are used by the signatory to sign.	APED Certification Practice Statement for Qualified Electronic Signatures, published at https://pki.aped.gov.gr/repository Policy ETSI EN 319 411-2 QCP-n-qscd

The Qualified Certificates for Electronic Signature are Long Term and valid for 3 years, while APED reserves the right to reduce the validity period of the Qualified Certificates for Electronic Signature.

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

3.1. The contract has a duration equal to the duration of validity of the "Document Signing - Qualified Certificates for Qualified Electronic Signatures with QSCD" issued to the Subscriber, which is three (3) years from their issuance and expires on the " validity expiration date" of the above certificates, which is listed in them. The obligations on both sides provided by the terms of this contract, the relevant APED Policy that applies after the expiration or revocation of the certificates, continue to be borne by the Subscribers.

3.2. Renewal of Qualified Certificates for Electronic Signature is not applicable but consists in re-creating certificate keys instead. Re-creation of certificate keys is the issuance of a new Qualified Certificate for Electronic Signature that certifies the new public key. Before Subscriber's existing certificate expires, Subscriber must regenerate keys for the certificate to ensure continued use of the certificate. Keys can be regenerated for the certificate even after it expires.

3.3. In the event of a violation of the terms of this contract or the relevant APED Policy by the Subscriber, or in any other case provided for in the relevant Policy, APED may revoke or suspend the Subscriber's Qualified Certificates for Electronic Signature (which is carried out with the addition of the certificate identification serial numbers to the published Certificate Revocation List, CRL, and also with the corresponding response of the OCSP server), informing the Subscriber accordingly. Also, revocation or suspension of the specific certificates is carried out by APED in the event that the latter is informed, in any convenient way, that the Subscriber no longer has real, legal and exclusive control of his private keys.

3.4. Revocation or suspension of the Qualified Certificates for Electronic Signature can and must be requested by the Subscriber himself (for his protection) in case of exposure of his keys or PIN to third parties, or after loss of the USB token, in which case APED must, after verifying the origin of the request, process it immediately.

4. Prohibitions of Use

4.1. Qualified Certificates for Electronic Signature are not designed, intended, or approved for use in situations where compliance with highly classified information or high security conditions (such as national defense and security) is required.

4.2. The Subscriber's Qualified Certificates for Electronic Signature are prohibited from being used outside of the limits and content specified in the CPS for Qualified Certificates for Electronic Signature of APED or for illegal purposes, or contrary to the public interest, or otherwise for a purpose that may harm the Greek State and the APED. By way of example, the use of Qualified Certificates for Electronic Signature is prohibited for any of the following purposes:

- Illegal activity (including cyber-attacks and attempted Certificate tampering)
- Issuance of a new Certificate and information about the validity of the Certificate
- Enabling other parties to use Subscriber's Private Key

- Facilitating the automated use of the Certificate issued for electronic signature
- Use of the Certificate issued for electronic signature to sign documents that may cause undesirable consequences (including signing such documents for test purposes)

5. Reliance Limits

5.1. Reliance Limits for Qualified Certificates for Electronic Signature

- Information in the Qualified Certificates for Electronic Signature is accurate. There are no errors or false statements as to the details of the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
- Qualified Certificates for Electronic Signature are valid from the date specified on the Certificate. The Certificate expires on the expiry date stated on the Certificate unless the Certificate is revoked
- Audit logs are kept within the system for at least two (2) months. Physical or digital records relating to Certificate applications, registration information and requests or applications for suspension, termination of suspension and revocation are kept for at least seven (7) years after the expiry of the relevant Certificate

5.2. Reliance Limits for Timestamps

- Timestamps are valid from the date specified in them. The Timestamp expires on the expiration date specified in the Timestamp unless the Certificate of the Timestamp Unit (TSU) is revoked. The Timestamp Authority (TSA) of APED ensures that the private signing keys of the TSU are not used beyond their end-of-life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place when the period of use of the TSU key expires and that the TSU private keys or any part thereof, including any copies, are destroyed in such a way that the private key cannot be recovered. The Timestamp Token (TST) generation system will reject any attempt to issue a TST if the private signing key has expired or if the private signing key period has expired
- ADEP has put technical procedures in place to ensure that Timestamp Tokens are issued securely and contain the correct time. APED's TSA ensures that its time is synchronized to UTC within the stated accuracy with multiple independent time sources. Timestamp Tokens are issued with an accuracy of ± one second. APED implements security controls that prevent unauthorized operation, in order to calibrate the time out of operation. APED ensures that synchronization is maintained when a leap second occurs.
- Timestamp Unit Certificates are valid for five (5) years. They are replaced every one (1) year. Timestamping Authority logs related to the Timestamp Unit Certificate are kept for seven (7) years after the expiration of the Timestamp Unit Certificate and Timestamping Authority logs related to the timestamp service are kept for at least one (1) year after the expiry of the TSU Certificate

6. Subscriber Rights and Obligations

6.1. Subscriber has the right to apply for a Qualified Certificate for Electronic Signature or request a Timestamp, upon acceptance of these Terms and Conditions and compliance with the requirements of the Certification Practice Statement of Qualified Certificates for Electronic Signature, as well as the Certification Policy and Certification Practice Statement of the Timestamp Authority of APED respectively.

The Subscriber must issue the Qualified Certificate for Electronic Signature within forty-five (45) days of its physical identification at the Authorized Office. After the expiry of this period the application is cancelled, and a new application must be submitted.

6.2. The Subscriber and/or Subject of the Qualified Electronic Signatures:

- is solely responsible for maintaining his Private Key
- is solely and fully responsible for any consequences from using his Certificate during and after the Certificate's validity
- is solely liable for any damage caused due to failure or undue performance of his obligations specified in the present Terms and Conditions and/or the law (National or European).
- should be aware that Electronic Signatures or Electronic Seals issued based on expired or revoked Certificates are invalid

6.3. The subscriber of a Qualified Electronic Signature shall:

- submit accurate, true and complete information regarding the issuance of the Qualified Certificate for Electronic Signature
- submit the necessary documents and supporting documents for his identification to APED as specified in the application form for the issuance of a Qualified Certificate of Electronic Signature, as well as follow the steps indicated by APED to complete the registration process
- not proceed with the process of issuing the Qualified Certificate of Electronic Signature, if the Subscriber does not have the legal right to do so, and/or is not an adult
- ensure that his Private Key is used under his control and exercise reasonable care to avoid unauthorized use thereof
- be responsible for the maintenance and ensuring of the secrecy of his Private Key when his Certificate is issued on Local QSCD, whereas he shall be responsible for the credentials (username, password, OTP) accessing the Private Key when his Certificate is issued on a Remote QSCD.
- use his Private Key and Certificate in accordance with present Terms and Conditions, including applicable agreements set out in Section 10, and the laws of Greece and European Union
- notify APED of the correct information within a reasonable time, in case of a change in his personal details or in case of any other inaccuracy in the content of the Qualified Certificate of Electronic Signature.
- immediately inform APED of the possibility of unauthorized use of his/her Private Key or if his/her Private Key has been lost, stolen, potentially compromised or if control of his/her

Private Key has been lost due to exposure to risk of the authentication credentials (e.g., PIN, PUK, User Code, Password, OTP) or for other reasons and immediately revoke the Qualified Certificate of Electronic Signature

- discontinue using his private key if the Qualified Certificate of Electronic Signature has been revoked or the Certification Authority has been exposed to risk

6.4. The Subscriber declares that he has been fully informed and knows everything about his rights and obligations, as well as all the possible conditions and risks of the electronic communication supported by the trust services provided by APED. Therefore, he acknowledges that his claim of loss of connection, leakage of PIN or inaccuracy of the certificate in general is invalid, unacceptable, abusive and contrary to good faith

6.5. The Subscriber accepts that, during the process of issuing / revoking the certificate, he will receive informative SMS on his certified mobile phone, which has been declared in the Application-Affirmation of gov.gr.

6.6. The Subscriber is solely responsible and obliged to compensate the damage of any third party who relied on his signature

6.7. The Subscriber must neither assign his rights nor transfer his obligations to third parties based on this Agreement. Any attempted assignment or authorization is invalid.

6.8. The subscriber of timestamp services shall:

- verify the signatures created by the Timestamp Authority of APED in Timestamp Token (Verification if signature of Timestamp Authority in Timestamp Token is valid and verification of Timestamp Authority's certificate)
- use secure cryptographic functions for timestamp requests
- know that expired timestamps are invalid

7. Obligations of APED

Without prejudice to Section 9, APED shall provide the trust services in accordance with the Certification Policy and the Certification Practice Statement.

7.1. APED is obliged:

- to create a pair of cryptographic keys following any procedure provided by the Policy
- to issue and manage personal certificates of type "Document Signing – Qualified Certificates for Qualified Electronic Signatures with QSCD" for the above key pairs of the Subscriber (i.e., an approved personal certificate) in compliance with the Policy
- to revoke the Qualified Certificate of Electronic Signature of the Subscriber when he requests it and to publish the Certificate Revocation List at regular intervals, as well as for the OCSP server to respond with the status of the Qualified Certificate of Electronic Signature, in accordance with the procedures and conditions of the relevant Policy of APED
- to publish the Policies it issues, as well as any modification thereof

- to provide continuous access to the electronic timestamp service except for special cases such as: planned technical interruptions, loss of synchronization time and other causes described in the relevant chapter of the Policy
- ensure that TimeStamping Units (TSUs) are coordinated to Universal Time (UTC) and have an offset of ± 1 second

7.2. APED guarantees to the Subscriber:

- the accuracy of all the information contained in the Qualified Certificate of Electronic Signature and the existence of all the data required for its issuance, in accordance with the relevant Policy of APED
- that the revocation of the Qualified Certificate of Electronic Signature will be published within 24 hours of the submission of the application, always in accordance with the conditions and procedures described in the APED Certification Regulation

7.3. APED operates the Provision of Trust Services in accordance with the Policy and the eIDAS and ETSI Regulations

7.4. The above guarantees are provided by APED only for use of its certificates and for use of timestamping service by the Subscriber, in accordance with the limitations and conditions specified in the relevant APED Policy

7.5. APED is not liable to anyone (subscriber or third party), if they are at fault or if their actions were not in accordance with the provisions of the relevant APED Policy. APED is not responsible for any malfunction of its services in cases of force majeure, such as earthquakes, floods, fires, etc., including cases of interruption of the electricity supply (black-out), problems in telecommunication networks and in general of all external obstacles that may prevent the smooth provision of its services and are not due to its fault.

7.6. APED is not responsible for any indirect or collateral damage, criminal or disciplinary prosecution or punishment, lost profits or any other indirect consequences caused to the subscriber due to the use or reliance on any of its certificates or the use of the electronic timestamping service. For the purposes of this paragraph, the term "damage" means partial loss or diminution in value as well as total loss

8. Obligations of Relying Parties

8.1. Each Relying Party studies the risks and responsibilities associated with accepting the Certificate. Risks and responsibilities are set out in the CPS and CP. A Relying Party acknowledges that it has access to sufficient information to ensure that it is able to make an informed decision about the extent to which it chooses to rely on the information in a Qualified Certificate. A RELYING PARTY IS RESPONSIBLE FOR DECIDING WHETHER TO RELY ON THE INFORMATION OF A QUALIFIED CERTIFICATE.

8.2. Each Relying Party acknowledges and agrees that its use of APED Repository and its reliance on any Qualified Certificate is governed by then-current CPS of APED. The applicable CPS is published in the online Repository at the address: https://pki.aped.gov.gr/repository. Amendments to the CPS are also published in the APED online Storage Space at the same address.

8.3. If there is insufficient information contained in the Certificate or Electronic Signature regarding the validity of the Certificate, the Relying Party shall verify the validity or revocation of the Qualified Certificate using the information of the current status of the Certificate based on the certificate validation services provided by APED at the time of the use of the Qualified Certificate or creation of a Qualified Electronic Signature. One method by which you can check the status of the Certificate is to refer to the most recent Certificate Revocation List from the Certification Authority that issued the digital certificate you wish to rely on.

8.4. The Relying Party follows the restrictions stated in the Certificate and makes sure that the transaction that is to be accepted complies with the CPS and the CP

- Qualified Certificates are used only to the extent that their use is in accordance with applicable law. APED Qualified Certificates are not designed, intended, or approved for use or resale as control equipment in hazardous conditions or for uses requiring fail-safe operation, such as in the operation of nuclear facilities, navigation, or aircraft communication systems, air traffic control systems or weapons control systems, where a failure could lead directly to death, personal injury or significant environmental damage.
- Timestamps will only be used to the extent that their use is in accordance with applicable law. Any restriction on the use of timestamps, indicated in the Certificate Policy & Certification Practice Statement of APED Timestamp Authority, should be taken into account. Subscribers and Relying Parties of Timestamp Services must verify the signatures created by the APED TSA in the TST. If the verification takes place after the Certificate has expired, they should follow the instructions in Annex D of ETSI EN 319 421.

8.5. APED ensures that the Trust Services are available on a 24/7 basis with a minimum total availability of 99% per year with planned outages not exceeding 0.4% per year.

8.6. The Relying Party verifies the validity of any Certificate issued by APED by checking the OCSP and CRL references found on the Certificate.

8.7. The Relying Party is expected to use a Trust List to determine whether an Electronic Signature or Timestamp is Qualified

9. Limited Warranty - Disclaimer - Limitation of Liability

9.1. APED is responsible for providing the Trust Services as defined in the Certification Policy and Certification Practice Statement for Qualified Electronic Signatures and Certification Policy and Certification Practice Statement of Timestamp Authority of APED

9.2. APED informs all Subscribers and Subjects before discontinuing the Certification service and maintains the documentation related to the discontinued Certification service as well as the information required according to the procedure set out in the CPS

9.3. APED is not liable for

- the confidentiality of the Subscriber's and Subject's Private Keys when they are stored in a local QSCD, for possible loss or destruction of the local QSCD

- any misuse of the Certificates or insufficient validity checks of the Certificates or for the incorrect decisions of a Relying Party or any consequences due to an error or omission of the Certificate validity check
- non-fulfilment of its obligations if such non-fulfilment is due to errors or security problems of the supervisory body, the Trusted Lists or other public authority
- failure to perform if such failure is due to force majeure

9.4. APED provides limited warranties and disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability and excludes all liability, excluding willful intent or gross negligence, for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising out of or in connection with the use, delivery, permission, fulfillment, non-fulfilment or unavailability of certificates, electronic signatures, time stamps or any other transactions or services provided or referred to herein, even if APED has been informed of the possibility of such damages

The Greek State is responsible for damage caused by acts or omissions of the APED bodies or the issuing CA to any natural or legal person, due to non-compliance with the obligations described in the CP and CPS, in accordance with article 105 of the Introduction Law of the Civil Code. Limitations of liability include the exclusion of indirect, special, incidental and consequential damages. In particular, the following apply for the responsibility of the Greek State due to actions or omissions of the bodies of the APED, in terms of compliance with the provisions of the present:

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

Besides, the provisions of paragraph 2 of article 13 "Responsibility and burden of proof" of regulation 910/2014 apply and apply in this case, pursuant to paragraph 3 of the same article.

9.5. Subscribers, Subjects and Relying Parties are hereby notified of the possibility of theft or other exposure of a private key corresponding to a public key contained in an authorized certificate, which may or may not be detectable, as well as of the possibility of using a stolen or compromised key to forge a qualified electronic signature on a document

9.6. APED 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. Without prejudice to paragraph 8.4, APED is not responsible for the forgery or authenticity of the identification documents nor for any damage caused to the Subscriber or to other persons due to them.

10. Applicable Agreements, Policies, CP, CPS

Relevant agreements, policies and practice statements related to the Terms and Conditions for the use of Qualified Trust Services are

10.1. Certification Policy of APED
10.2. APED Certification Practice Statement for Qualified Certificates for Electronic Signatures
10.3. Certificate and OCSP Profiles for Qualified Electronic Signatures and specifically:
- Policy of Root CA certificate (1.2.300.0.110001.2)
- Policy for Qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD (1.2.300.0.110001.2.1.1)
- Normalized Certificate Policy (OID 0.4.0.2042.1.1)
- Normalized Certificate Policy requiring a secure cryptographic device (OID 0.4.0.2042.1.2)

10.4. Time Stamping Authority Certificate Policy & Certification Practice Statement of APED
10.5. Privacy Statement of APED

Current versions of all above applicable documents are published at https://pki.aped.gov.gr/repository

11. Privacy Policy and Confidentiality

11.1. APED adheres to the Privacy Policy, which is included in the APED Repository at https://pki.aped.gov.gr/repository and European Union legislation, when processing personal information and logging information
11.2. All information that has become known while providing services and that is not intended for disclosure (e.g., information that APED has become aware of from operating and providing Trust Services) is confidential. Subscriber and Subject have the right to be informed about the information that APED maintains for them, pursuant to the law. The categories of information considered Confidential are detailed in CP and Privacy Policy of APED.
11.3. APED secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties
11.4. APED has the right to disclose information about Subscriber or Subject to third parties who pursuant to relevant legislation are entitled to receive such information.
11.5. Additionally, non-personalized statistics on the services of APED are also considered public information. APED may publish non-personalized statistical data about its services.

12. Refund Policy

APED provides Trust Services defined in the CP at no cost.

13. Applicable law, complaints and dispute resolution

13.1. Disputes between APED, issuing CAs, Subscribers and Relying Parties will be resolved in accordance with applicable law governing the relationship between the parties.

13.2. To the extent permitted by law, before any dispute resolution mechanism may be invoked with respect to a dispute involving any aspect of APED Trust Services, the Subscriber or any other interested party must notify APED and any other party involved in the dispute of any claim or complaint, not later than thirty (30) calendar days after the detection 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 interested party may seek court resolution. All parties agree that the courts of Athens, Greece, shall have exclusive jurisdiction and are competent to resolve any dispute regarding the interpretation and application of these Terms and the provision of the services of APED.

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

14. Licenses, Trusted List and Audit

14.1. APED is a Qualified Trust Service Provider granted the status of Qualified provider by the supervisory body (EETT) and included in the EU Trusted List, following the submission of a conformity assessment report by an accredited Conformity Assessment Body

14.2. Trust Services of APED for Qualified Electronic Signatures are registered in the European Trust List of Qualified Trust Service Providers (List of Trusted Lists - LOTL). The European Trust List of Qualified Trust Service Providers is available at the following link: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home. The requirement of the above registration is in accordance with Regulation (EU) No 910/2014.

14.3. The Conformity Assessment Body has been accredited in accordance with Regulation (EC) No. 765/2008 as being able to assess the compliance of Qualified Trust Service Providers and Qualified Trust Services that they provide.

14.4. The conclusions of the controls or the certificates, which are based on the results of a conformity assessment audit carried out in accordance with the eIDAS regulation, the corresponding legislation and standards, are published on the APED website at the address: https://pki.aped.gov.gr/repository

15. Contact Details

Contact details of APED 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 APED Certification Regulation in the Government Gazette. Then, this text is immediately published in the repository of APED.

16.2. These Terms and Conditions will remain in effect until superseded by any new, amended version. Modified or new versions are listed in the repository of the APED

16.3. With the repeal of CP of APED, SubCAs, Subscribers and Dependent Parties of Public Key Infrastructure of APED are still bound by its terms, with regard to all certificates issued during the validity of this CP and for the remainder of their period of validity

16.4. If any provision of these Terms and Conditions, or the application thereof, is for any reason found to be invalid or unenforceable, the remainder (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability and shall be interpreted in a manner that shall reasonably fulfil the intent of the parties.

16.5. The present Terms and Conditions are drafted in English and Greek versions. In case of any discrepancies between these versions, the Greek version will prevail.

17. Processing of Personal Data

17.1. The subscriber gives APED his express and unconditional consent to collect, control, process and archive his personal data, which are necessary for the provision of trust services. This processing of personal data is carried out in compliance with the provisions of the relevant institutional framework (new General Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016 "on the protection of natural persons against the processing of personal data and for the free movement of such data", GDPR, Law 3471/2006, Law 2472/1997 etc.) and these data will not be used for other purposes, without the express consent of the subscriber

17.2. This personal data is collected exclusively by the subscribers themselves during the subscription registration process and is kept for a period of at least 7 years from the expiry of the certificates, in order to be used in particular to provide evidence in dispute resolution procedures related to the certification of electronics signatures of the subscriber. The subscriber expressly declares that he is aware of, accepts and consents to the above processing of his personal data, as well as that he authorizes APED (or its possible successor in the provision of the relevant services) to disclose his personal data to third parties in any dispute resolution process related to the use of its certificates

17.3. In any case, the subscriber has the right to turn to APED (which in this case is the "Data Controller" according to the law), to make use of the "Information" (Articles 12, 13 and 14 of the GDPR), "Access" (Article 15 GDPR) and "Portability" (Article 20 GDPR) rights.