Hellenic Public Administration Certification Authority (APED)

Certification Regulation

(CP-CPS)

As amended and valid

[Gazette B' 2403/24-4-2024]

Latest Update: 24-4-2024

Contents

Having regard to: 7
Version History 8
1. Introduction 9
2. Certification Regulation of the Hellenic Public Administration Certification Authority (APED) 10
A. Certificate Policy of APED 10
1. Introduction 10
1.1. Overview 11
1.2 Document name and Identification 11
1.3 PKI Participants 12
1.4 Certificate Usage 13
1.5 Policy Administration 13
1.6 Definitions and Acronyms 14
2. Publication and Repository 14
2.1 Repositories 14
2.2 Publication of Certificate Information 14
2.3 Time or Frequency of Publication 14
2.4 Access Controls on Repositories 15
3. Identification and Authentication 15
3.1 Naming 15
3.2 Initial Registration 16
3.3 Identification and Authentication for Re-keying Requests 19
3.4 Identification and Authentication for Revocation Request 19
4. CERTIFICATE LIFE-CYCLE OPERATIONAL 20
4.1 Certificate Issuance Application 20
4.2 Certificate Issuance Application Processing 21
4.3 Certificate Issuance 21
4.4 Certificate Acceptance 22
4.5 Key Pair and Certificate Usage 22
4.6 Certificate Renewal 23
4.7 Certificate Re-Key 23
4.8 Certificate Modification 24
4.9 Certificate Revocation 24
4.10 Certificate Status Services 26
4.11 End of Subscription 26

5. Physical, Management and Operational Protection and Security Measures 26
5.1 Physical Controls 27
5.2 Procedural Controls 28
5.3 Personnel Controls 28
5.4 Audit Logging Procedures 30
5.5 Records Archival 31
5.6 Key Changeover 32
5.7 Compromise and Disaster Recovery 32
5.8 CA or RA Termination 33
6. Technical Security Controls 34
6.1 Key Pair Generation and Installation 34
6.2 Private Key Protection 35
6.3 Other Aspects of Key Pair Management 37
6.4 Activation Data 37
6.5 Computer Security Controls 38
6.6 Life Cycle Technical Controls 38
6.7 Network Security Controls 38
6.8 Time-Stamping 38
7. Certificate, CRL and OCSP Profiles 39
7.1 Certificate Profile 39
7.2 CRL Profile 41
7.3 OCSP Profile 41
8. Compliance Audit and Other Assessments 42
8.1 Frequency of Assessment 42
8.2 Identity/Qualifications of Assessor 42
8.3 Assessor's Relationship to Assessed Entity 42
8.4 Topics Covered by Assessment 42
8.5 Actions taken as a Result of Deficiency 42
8.6 Communication of Results 43
9. Other Business and Legal Matters 43
9.1 Fees 43
9.2 Liability 43
9.3 Confidentiality of Information 44
9.4 Privacy of Personal Information 44
9.5 Intellectual Property Rights 45
9.6 Representations and Warranties 45

9.7 Disclaimers of Warranties 46
9.8 Limitations of Liability 46
9.9 Duration and Termination 46
9.10 Individual Notices and Communications with Participants 46
9.11 Amendments 46
9.12 Posting and Communication Policy 47
9.13 Dispute Resolution 47
9.14 Applicable Law 47
9.15 Force Majeure 47
B. Certification Practice Statement of Subordinate Certification Authorities of the Hellenic Public Administration Certification Authority 48
1. Introduction 48
1.1 Summary 48
1.2 Document Name and Identification 49
1.3 PKI Participants 49
1.4 Certificate Usage 51
1.5 Policy Administration 51
1.6 Definitions and Acronyms 51
2. Publication and Repository 51
2.1 Repositories 51
2.2 Publication of Certificate Information 51
2.3 Time or Frequency of Publication 52
2.4 Access Controls on Repositories 52
3. Identification and Authentication 52
3.1 Naming 52
3.2 Initial Registration 53
3.3 Identification and Authentication for Re-keying Requests 53
3.4 Identification and Authentication for Revocation Request 53
4. CERTIFICATE LIFE-CYCLE OPERATIONAL 54
4.1 Certificate Issuance Application 54
4.2 Certificate Issuance Application Processing 54
4.3 Certificate Issuance 54
4.4 Certificate Acceptance 55
4.5 Key Pair and Certificate Usage 55
4.6 Certificate Renewal 55
4.7 Certificate Re-Key 55

4.8 Certificate Modification 55
4.9 Certificate Revocation 56
4.10 Certificate Status Services 57
4.11 End of Subscription 57
5. Physical, Management and Operational Protection and Security Measures 57
6. Technical Security Controls 57
7. Certificate, CRL and OCSP Profiles 57
8. Compliance Audit and Other Assessments 57
9. Other Business and Legal Matters 57
9.1 Fees 57
9.2 Financial Responsibility 57
9.3 Confidentiality of Information 57
9.4 Privacy of Personal Information 57
9.5 Intellectual Property Rights 57
9.6 Representations and Warranties 58
9.7 Disclaimers of Warranties 58
9.8 Limitations of Liability 58
9.9 Duration and Termination 58
9.10 Individual Notices and Communications with Participants 58
9.11 Amendments 58
9.12 Posting and Communication Policy 58
9.13 Dispute Resolution 58
9.14 Applicable Law 58
9.15 Force Majeure 58
C. Certificate Policy & Certification Practice Statement for Time Stamping Services 59
1. Introduction 59
2. General Concepts 59
2.1 Time Stamping Services 59
2.2 Time Stamping Authority 59
2.3 Subscribers 60
2.4 Time Stamping Policy and TSA Practice Statement 60
3. Time Stamp Policies 61
3.1 Overview 61
3.2 Identification 61
3.3 User Community and Applicability 61
3.4 Conformance 61

4. Obligations and Liability 61
4.1 TSA Obligations towards Subscribers 61
4.2 Subscriber Obligations 62
4.3 Relying Party Obligations 62
4.4 Liability 62
5. Certification Practice Statement of TSA 63
5.1 Practice and Disclosure Statements 63
5.2 Key Management Life Cycle 64
5.3 Time Stamping 65
5.4 TSA Management and Operation 65
APPENDIX A – References, Acronyms and Definitions 68

Having regard to:

1. The provisions of:
   a. Regulation (EU) 910/2014 of the European Parliament and the Council of July 23rd, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (L 257/73).
   b. Regulation (EU) 2016/679 of the European Parliament and the Council of April 27th, 2016 on the protection of natural persons against the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/ EC (General Data Protection Regulation).
   c. Law 4727/2020 "Digital Governance (Incorporation into Greek Law of Directive (EU) 2016/2102 and Directive (EU) 2019/1024) - Electronic Communications (Incorporation into Greek Law of Directive (EU) 2018/1972) and other provisions", and in particular Chapter IX and par. 37 of article 107 of this law (A' 184).
   d. Law 4624/2019 "Personal Data Protection Principle, measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons against the processing of personal data and incorporation into national legislation of Directive (EU) 2016/680 of the European Parliament and the Council of April 27th, 2016 and other provisions (A'137)".
   e. Presidential Decree 40/2020 "Organization of the Ministry of Digital Governance".
   f. Presidential Decree 77/2023 "Establishment of a Ministry and renaming of Ministries - Establishment, abolition and renaming of General and Special Secretariats - Transfer of responsibilities, service units, staff positions and supervised bodies" (A' 130).
   g. Presidential Decree 79/2023 "Appointment of Ministers and Deputy Ministers" (A΄ 131).
   h. Article 90 of the Code of Legislation for the Government and Government Bodies, (Presidential Decree 63/2005 - A' 98), in conjunction with par. 22 of article 119 of Law 4622/2019 (A' 133).
2. Decision No. 245/5.1.2022 of the Minister of State "Commencing the operation of the Hellenic Public Administration Certification Authority (APED)". (B΄43)
3. Decision No. 243/5.1.2022 of the Minister of State "Certification Regulation of the Hellenic Public Administration Certification Authority (APED)". (B΄43)
4. Decision No. 2051/19.1.2023 of the Ministers of Digital Governance and State "Definition of organic units of the Hellenic Public Administration Certification Authority (APED)." (B΄ 216)
5. Decision No. 837/1B/30.11.2017 of the Hellenic Telecommunications and Post Commission (EETT) "Regulation on the Provision of Trust Services" (B' 4396).
6. Decision No. 1012/03/25.10.2021 of EETT "Evaluation of compliance of the services for issuing of Qualified Certificates of Electronic Signatures and Qualified Electronic Time Stamps of the "Hellenic Public Administration Certification Authority (APED)", according to which the compliance of APED with the requirements of EU Regulation 910/2014 (eIDAS) is ascertained.
7. The fact that the issuance of the present Ministerial Decision does not burden the state budget.
8. The need to ammend the terms and conditions for the provision of trust services by the Hellenic Public Administration Certification Authority (APED) as a qualified provider, in accordance with the provisions of EU Regulation 910/2014 (eIDAS), in order to upgrade the services it provides, namely:
   a. Remote identification service,
   b. Connection with Civil Registry,
   c. Revocation of certificate in case of application failure, due to a sudden and unforeseeable event and
   d. Issuance of qualified electronic signature certificates based on a remote device (Qualified Signature Creation Device).

Version History

Date	Version	Changes
15/12/2021	1.0	Initial document
24/4/2024	1.1	Addition of remote authentication service, remote QSCD, interoperability with civil registry, typo fixes

1. Introduction

The present Ministerial Decision constitutes the Certification Regulation of the Hellenic Public Administration Certification Authority - APED, of article 58 of Law 4727/2020, as amended by Article 164 of Law 4808/2021, which defines the terms and conditions for the provision of trust services from APED, whose structure includes the Primary Certification Authority (PCA), the Subordinate Certification Authorities (SubCA), the Registration Authorities and the Local Registration Authorities, for the purpose of generally providing trust services of the Greek State, through of the APED Public Key Infrastructure, which is analyzed in the individual chapters herein. APED is responsible for issuing and managing certificates for the provision of trust services to all public sector bodies, as well as to natural or legal persons or legal entities.

The Certification Regulation defines the APED Certificate Policy (Section A), the Practice Statement of the Subordinate Certification Authorities of the APED (Section B), specifies the terms and conditions for the provision of Qualified Trust Services in accordance with the APED Certificate Policy and additionally defines the Certificate Policy and Practice Statement of the (Subordinate) Time Stamp Authority (Section C).

In particular, the trust service certificates of APED are electronic certificates, with which:

a. The owner can use trust services and
b. The owner of the certificate is identified through the confirmation of his name or nickname.

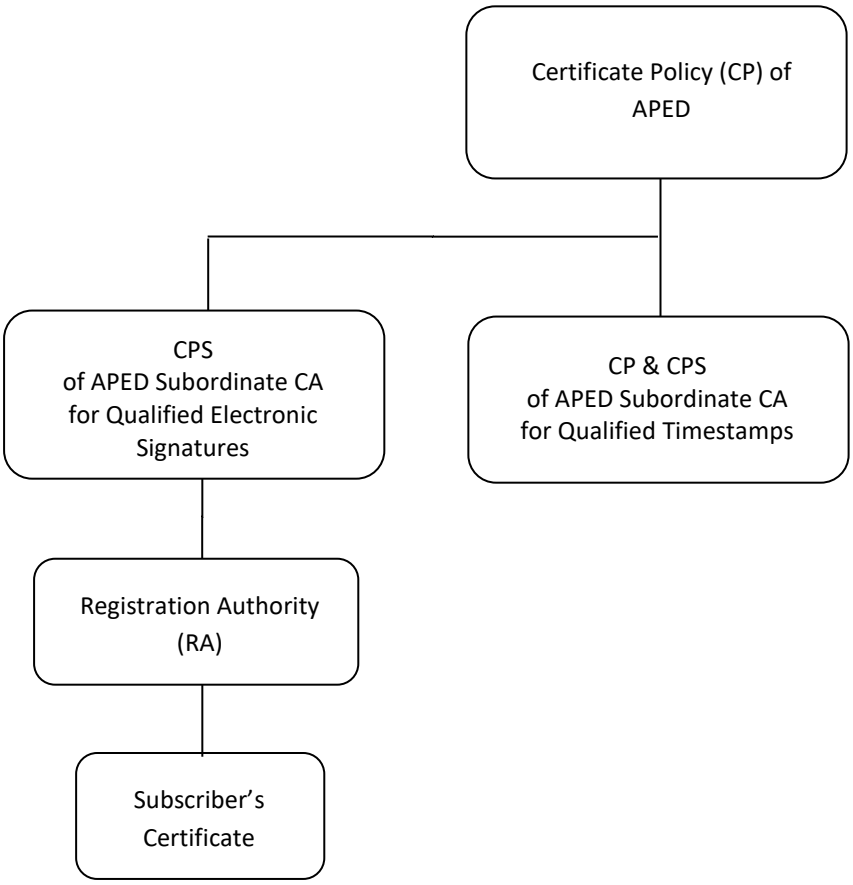
The content and requirements of the qualified certificates are defined in the eIDAS Regulation and its Annexes, while the validity of the certificate starts from the date written on it and in any case no earlier than the registration of the owner's data, during the electronic identification process of article 57 of Law 4727/2020, in the database maintained by the trust service provider. Finally, the certificate expires:

a. upon expiry date written on it, or
b. upon revocation of the certificate in accordance with article 55 of the same law.

The present document is drafted in English and Greek versions. In case of any discrepancies between these versions, the Greek version will prevail.

2. Certification Regulation of the Hellenic Public Administration Certification Authority (APED)

This Regulation defines the Certification Policy of APED as well as the Practice Statement of the Subordinate Certification Authorities. The hierarchy of the Public Key Infrastructure (PKI) of APED is illustrated in the figure below.



It is noted that the term SubCA and Issuing CA refers to the Certification Authorities which have APED as Primary (Root) Certification Authority

A. Certificate Policy of APED

1. Introduction

This Certificate Policy (CP) defines the certificate policy of APED, the terms and conditions for the assignment and support or provision of trust services to entities - Trust Service Providers, who are required to apply this legal, technical and operational framework of trusted services.

In any case, APED ensures and takes the necessary measures for the implementation of this CP in its areas of responsibility, as described in this text.

1.1. Overview

The present CP defines the terms, conditions for issuing, maintaining and managing the life cycle of qualified certificates for electronic signatures and electronic time stamps and the provision of the relevant trust services by issuing CAs. In particular, this CP sets the framework for:

- The obligations of issuing Certification Authorities, Registration Authorities, Subscribers (End Users) and Relying Parties.
- The issues related to the General Terms and Conditions of Use of Certificates.
- The methods used to confirm the identity of Subscribers.
- Operational procedures for Certificate lifecycle services: request for issuance, acceptance and revocation of Certificatekeys.
- The contents of Certificates, Certificate Revocation Lists (CRLs), and Online Certificate Status Protocol (OCSP) Certificates, when available.
- Security operational procedures for audit logging, record keeping and disaster recovery.
- Physical security, personnel security, key management and logical security regulations.
- The management of the CP, including its modification methods.
- The technical specifications and specializations of the Practice Statements of the Subordinate Certification Authorities of APED.

Table 1 includes the list of APED documents to be published, as well as their publication locations. Documents not available for publication are confidential material of APED.

Table 1: Available Regulation Documents

Documents	State	Publication Location
Certification Regulation of APED	Public	Repository of APED, according to §2.2 of CP
Terms and Conditions of Certificate Usage	Public	Repository of APED, according to §2.2 of CP

1.2 Document name and Identification

APED has adapted this CP to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, also known as RFC 3647, of the Action Group for the Internet Engineering Task Force, a body responsible for setting standards on the Internet, to facilitate the depiction of the certificate policy in place. Small deviations from the structure of RFC 3647 in individual details are necessary due to the application of the operational model of the APED in the public sector. APED, furthermore, reserves the right to take the necessary actions within the framework of this CP, where this is deemed appropriate, in order to improve the quality of its services.

1.2.1 Policy of Qualified Certificates of Electronic Signatures

This Certificate Policy refers to Qualified Certificates of Electronic Signatures of subscribers

Certificates issued on the basis of this CP are suitable to support a qualified electronic signature (according to paragraph 12 of article 3 of EU Regulation 910/2014 (eIDAS)), which is based on a Qualified Certificate and created by a Qualified Signature Creation Device (QSCD), in which case it bears the state of physical signature in both substantive and procedural law, in accordance with article 25 of the above Regulation and articles 14, 15, 16 and 50 of Law 4727/2020.

The CP corresponds to the "QCP-n-qscd" public certificate policy as described in the ETSI EN 319 411-2 *V2.5.1 (2023-10)* standard of the European Telecommunications Standards Institute - ETSI regarding the Policy Requirements for Certification Authorities issuing Qualified Certificates. The Certificates issued on the basis of the CP certify the

correspondence of the natural person (Subscriber) with the information mentioned in his identification document. The above standard is also used in the case of issuing qualified electronic signature certificates using a remote QSCD.

The identification of the Subscribers requires their physical presence before competent officials in accordance with the provisions of this act, who check the documents verifying the identity of the Subscriber (§3.2.2). Besides, identification can take place remotely, as long as the terms and conditions of no. 27499/2021 Decision of the Minister of State (Government Gazette 3682/B'/10-8-2021).

Qualified Certificates of Subscribers refer exclusively to natural persons. In any case, the Qualified Certificate is linked exclusively to a natural person, who bears the sole responsibility for this certificate.

The Certificate Policy Identifier corresponding to the Certificate Policy is: 1.2.300.0.110001.2.1.1.

1.3 PKI Participants

This CP governs the Public Key Infrastructure services provided by APED

1.3.1 Certification Authorities

APED may include in the present Public Key Infrastructure other public services or bodies of the public sector (Subordinate Certification Authorities), which follow the Certificate Policy of APED.

Subordinate Certification Authorities (SubCAs) which are designated by Joint Ministerial Decision of the Ministry of Digital Governance and the competent Minister and join the Public Key Infrastructure, based on Law 4727, art. 107, par. 37 and the provisions herein, are checked by the Conformity Assessment Body (CAB), approved by EETT and, if required, registered in EETT's Trust List. The certificates that will be issued by SubCAs will be managed by APED.

One or more organizational units are designated by similar Joint Ministerial Decision of the Ministry of Digital Governance and the competent Minister which, after being notified to APED, will exercise the responsibilities of the "Registration Authorities" and the "Local Registration Authorities" (CP §1.3.2 and CP §1.3 .3). The SubCAs can also exercise the responsibilities of the Registration Authority and the Local Registration Authorities as defined in sections §1.3.2 and §1.3.3.

1.3.2 Registration Authorities

In the process of granting qualified certificates for electronic signatures in accordance with the provisions herein, Registration Authorities (RA) are responsible for checking the requests and registrations of the Subscribers, and for confirming identity information of the Subscribers. In addition, the CAs control and recommend the issuance and revocation of Certificate keys.

1.3.3 Local Registration Authorities (LRA)

Each Registration Authority is addressed by a number of Local Registration Authorities, whose officers are responsible for confirming - verifying the identity of Subscribers as well as receiving requests for issuance and revocation of Certificate keys and report to the Registration Authority (or Authorities) in charge.

1.3.4 Subscribers (End Users)

Subscribers (End Users) are natural persons, holders of Certificates in accordance with the provisions herein. For certificates issued according to the CP in particular, Subscribers should have legal capacity.

1.3.5 Relying Parties

Relying Parties are natural or legal persons acting in reliance on a Certificate issued in accordance with the provisions herein. The Relying Party may be, or may not be, a Subscriber within the PKI of APED.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

Certificates that follow the CP in accordance with the provisions herein, are Qualified Certificates for Electronic Signature within the meaning of paragraph 15) of article 3 of Regulation 910/2014.
The Subscriber Certificates issued for natural persons are strictly personal and are used in the context provided by the Certification Practice Statements of SubCAs.

Applications, in which the Subscriber Certificates that may be used will be provided based on the Public Key Infrastructure herein and using a qualified electronic signature, where required, may be exclusively one or more of the following:

- Security access
- Secure identification of signer
- Identification of the person responsible for each relevant electronic communication / transaction
- Signing electronic files (eg Adobe Acrobat files)

1.4.1.1 Restrictions on the use of certificates

Certificates issued in accordance with the CP have restrictions on their use as defined in §1.4.1 hereof. In any case, the provisions herein do not affect provisions that, with regard to the conclusion and validity of contracts or legal obligations in general, do not impose the use of a certain type, nor do they affect provisions on the evidentiary or other use of documents or provisions by which it is prohibited to documents of certain categories and/or personal data are circulated and become known.

1.4.2 Prohibited Certificate Uses

Certificates 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. Moreover, the use of the Certificates for purposes other than those for which they were strictly issued is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is issued and amended by APED, as Root Certification Authority. Any requests for clarifications on the chapters herein will be addressed to APED.

1.5.2 Contact Information

Contact information for APED is published at https://www.aped.gov.gr

1.5.3 Eligibility Approval of Certification Practice Statements

APED examines and approves the Certification Practice Statements of SubCAs regarding their suitability and compliance in technical, procedural and related matters, with the requirements herein. Amendments to approved Certification Practice Statements also require the prior approval of APED.
Amendments to the present document require re-compliance of issuing CAs, within a period of time determined by APED, and approval by APED of each Practice Statement.

1.5.3.1 CPS Approval Procedures

The APED takes the necessary measures, has the appropriate mechanism and means for the processing and control of compliance of the Practice Statements of the issuing CAs, as well as their possible amendments with this CP.

1.6 Definitions and Acronyms

See chapter 3, Appendix A for table of Sources, Definitions and Acronyms

2. Publication and Repository

2.1 Repositories

APED ensures the operation of an electronic storage space for the Root Certification Authority. Issuing CAs shall also ensure a publicly accessible electronic repository for the PKI services they offer.

APED ensures that its storage space is available 24 hours a day, 7 days a week, with a minimum total availability of 99.00% per year with planned outages not exceeding 0.3% per year. In the event of system failure, maintenance work or other factors beyond the control of APED, every effort will be made to ensure that the unavailability of the specific information service does not exceed the time stated above.

2.2 Publication of Certificate Information

Both the CA and issuing CAs maintain a publicly accessible repository located on a network node that allows Relying Parties to check the status of Certificates by issuing Certificate Revocation Lists (CRLs).
APED issues Certificate Revocation Lists for SubCAs, while each issuing CA issues Certificate Revocation Lists for the subscriber Certificates it has issued.

With the revocation of a Certificate of Authority, APED publishes an announcement of this revocation in their storage area. Upon revocation of a Subscriber Certificate, issuing CA immediately publish this revocation in accordance with the mechanisms provided for in this CP (§4.9.6 and §4.9.8). For this purpose, issuing CAs may also provide online certificate status checking services in real time (Online Certificate Status Protocol - OCSP).

APED publishes this CP in the storage space located on its network node. Each issuing CA publishes this CP, its Certification Practice Statement, the Terms and Conditions of Certificate Use in the storage space located on its network node.

Finally, issuing CAs publish the Subscriber Certificates they approve, provided that:

- this is necessary for the purpose of using the Certificates, and
- no relevant limitation is imposed by the current legislation on the protection of personal data.

In the event that the above conditions are met, issuing CAs provide Relying Parties with information about the publication location and how to search for the Subscriber Certificates they issue.

2.2.1 Publication of CP

This CP is published in electronic form at the APED Repository at https://pki.aped.gov.gr/repository, where it is available in Adobe Acrobat® document format.

2.2.2 Items not published in the CP

Security documents considered confidential by APED are not disclosed to third parties.

2.3 Time or Frequency of Publication

APED announces the modifications of the CP, within a period of 30 days, in the section of its Storage Space intended for Policy Updates and Announcements, at the addresses mentioned in section §2.2.1. Subscriber Certificates are published upon issue, in accordance with §2.2. Information regarding the status of Certificates is published in accordance with §4.9.6 and §4.9.8 of the CP.

2.4 Access Controls on Repositories

APED ensures the application and implementation of logical and physical security measures in order to prevent the addition, deletion or modification of entries in the storage space by unauthorized persons. This is also an obligation for issuing CAs regarding their storage space.

APED and issuing CAs do not use technical means to restrict access to this CP and their own Certification Practice Statements, Certificates, and Certificate status information or CRLs etc. However, issuing CAs may require from third parties the prior acceptance of the Terms and Conditions of Certificate Use, as a condition for the use of Certificates, Certificate status information or CRL.

3. Identification and Authentication

3.1 Naming

The names appearing on the Certificates, which comply with the APED Certificate Policy, are verified.

3.1.1 Type of Names

The Certificates issued by the APED for the certification of the SubCAs, include X.501 Distinguished Names in the Issuer and Subject fields. The Distinctive Names of the SubCAs of APED consist of the elements specified below in Table 2

Table 2: Distinctive Name of SubCA

Χαρακτηριστικό	Τιμή
Country (C) =	"GR"
Organization (O) =	“HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY”
Common Name (CN) =	The Common Name of the SubCA (CA name): "APED Qualified eSignature Issuing CA".

Subscriber Certificates issued in accordance with the certification policies defined in this CP include a X.501 distinctive name in the Subject name field and consist of the elements specified in Table 3. The values that are included in individual fields are specified in the Certification Practice Statement of the CA, where this is deemed necessary.

Table 3: Elements of Distinctive Name of Subscriber Certificate

Χαρακτηριστικό	Τιμή
Country (C) =	"GR"
Common Name (CN) =	This attribute includes the first and last name (one or more) of the Subscriber
Surname (SN) =	This attribute includes the last name (one or more) of the Subscriber with Latin characters (using the ELOT 743 standard, unless stated differently on the identification document presented at registration)
Given name (G) =	This attribute includes the name (or names) of the Subscriber in Latin characters (using the ELOT 743 standard, unless it is written differently in the identification document presented during registration).
Serial Number =	This attribute includes the Subscriber's Certificate Serial Number according to the ETSI EN 319 412-1 standard

3.1.2 Need for Names to be Meaningful

The names included in the Subscriber Certificates are in a simple and comprehensible form to allow identification of the natural person who is the Subject of the Certificate.
CA Certificates of APED include names with widely understood semantics, making it possible to identify the CA that is the Subject of the Certificate

3.1.3 Anonymity or Pseudonymity of Subscribers

Not applicable.

3.1.4 Uniqueness of Names

Issuing CAs of APED ensure Subject Distinguished Names (DN) of Subscriber are unique through automated components of the Subscriber enrollment process.
The uniqueness of the Distinguished Name for electronic signatures and authentication is ensured by the Serial Number attribute value in the Subject field of the certificate.

3.2 Initial Registration

Identity validation is part of the process of the certificate application and certificate issuance

3.2.1 Method to Prove Possession of Private Key

The Certificate applicant must demonstrate that she/he rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be according to PKCS #10 (Public-Key Cryptography Standards) or another cryptographically equivalent demonstration or another approved method by APED.

3.2.2 Authentication of Identity of Natural Person

For all Certificates of natural persons, the competent Registration Authority and/or issuing Certification Authority, confirm that:

- Subscriber is the person identified in the Online Registration or Certificate Application.

Certification of the Subscriber's identity (identification) is performed by his personal (physical) presence before an official of the Local Registration Authority (LRA), or where this is deemed necessary, before the Registration Authority, or of the Issuing CA, for the purpose of checking identity information. Alternatively, identification is performed remotely, as long as the terms and conditions of no. 27499/2021 Decision of the Minister of State (Government Gazette 3682/B'/10-8-2021) are met.

- Acceptable identification documents for physical identification are:
  i. Police Identity Card (Greek or another European Union state)
  ii. Greek Military (Army, Navy, Air Force, Security Forces)
  iii. Passport.
- Acceptable identification documents for remote identification are the following, provided that they meet the conditions of article 4, par 1, 2 no. 27499/2021 Decision of the Minister of State (Government Gazette 3682/B'/10-8-2021):
  i. Police Identity Card (Greek or another European Union state)
  ii. Greek Military (Army, Navy, Air Force, Security Forces)
  iii. Passport.

  Especially for the period until 24/9/2024, valid police identity cards are accepted, in which the name is also written in Latin characters (GRC-BO-01004, GRC-BO-01005, GRC-BO-02001), identity cards of the officers of the Armed Forces and the Security Forces

The identification process is described below:

- The subscriber is informed in detail about the procedure at https://www.aped.gov.gr. There are links to two initial steps:
  - (1) link in the application –Declaration at gov.gr,
  - (2) link to the portal https://services.aped.gov.gr/apedcitizen/login/
- The subscriber navigates to gov.gr to the application – Declaration for the issuance of a Qualified Certificate and creates it.

- The application – Declaration form on gov.gr has a standard text. The user selects the form, is then authenticated (two-factor authentication, using the certified mobile phone), fills in the identification fields and creates it.
  - The application includes additional sections (text only): information on personal data processing, and some basic terms of use and reference to the text of the terms of use.

- The subscriber submits the ”application at the APED portal”.
  - The citizen gains access to the electronic application at the portal https://services.aped.gov.gr/apedcitizen/login/ using the credentials available through the General Secretariat of Information Systems and Digital Governance (G.S.I.S.D.G.) of the Ministry of Digital Governance.
  - Submits a request for the issuance of a Qualified Certificate.
    - The basic fields are pre-filled (retrieval from the AADE web service).
    - The subscriber fills in optional contact information: email, home address.
    - The subscriber fills in the unique verification identification number (code) of the gov.gr application-Declaration.
    - The subscriber chooses:
      i. Identification with physical presence or
      ii. Remote Identification
    - The subscriber is asked to confirm (check) that he has read the terms of use.
    - Submits the electronic application ("application at the APED portal"). A check is automatically made on the basic fields (name, surname, Taxpayer Identification Number - TIN) between retrieved AADE data and gov.gr application-Declaration. The electronic request and the gov.gr application-Declaration are stored in the database.

- The following two cases exist:
  i. Identification with physical presence
    - The subscriber goes to any LRA Office for physical identification.
    - The LRA officer is authenticated in the APED portal with the use of the Public Administration credentials of the General Secretariat of Information Systems and Digital Governance of the Ministry of Digital Governance, in accordance with what is defined in No. 29810 /23.10.2020 decision of the Minister of State, for the case of Public Servants, or else with the use of the TaxisNet credentials of the General Secretariat of Information Systems and Digital Governance of the Ministry of Digital Governance.
    - The LRA officer searches and locates the subscriber. He is navigated to the application details page. From there he can see the application-Declaration of gov.gr.
    - The LRA officer identifies the subscriber and confirms the correctness of the details of the gov.gr application.
    - The LRA officer also makes a comparison between the retrieved data from the Tax Registry of AADE/GSISDG (name, surname, TIN) and the corresponding data in the application – Declaration of gov.gr. If there is no match, the request is cancelled.
    - The employee corrects, if necessary, the editable fields (name-surname (Latin), address, email). The Latin spelling of the name shall be the same as that mentioned in the identification document.
    - The identifier of the identification document (identity card or passport) is automatically entered by the application - Declaration of gov.gr. The identification document must be the same as the one that the subscriber has entered in the application - Declaration of gov.gr and it is either a police ID (Greek or of another European Union state) or a Greek Military ID or a passport.
    - The application for Qualified Certificate has a unique identifier (similar to a protocol number) which is displayed to the LRA officer. Neither the application for Qualified Certificate nor a receipt is printed.
    - The LRA officer chooses to submit the request. If the identification document is a Greek Police ID or a Greek Passport, it is checked through the Interoperability Center at the Police ID Card Registry

or the Passport Registry, respectively, of the Greek Police. If it is a Greek Military ID (Army, Navy, Air Force, Security Forces), as long as the relevant service has been integrated into the application, a verification is made through the Interoperability Center, with the corresponding register of Military IDs

- If the verification is successfully completed or another identification document is used, for which no verification service is available, the LRA officer digitally signs the subscriber's Attestation of Physical Identification.
- The physical identification process is completed if and only if the verification of the identification document determines that the identification document is active (in the categories of documents that fall under this verification) and the relevant Attestation is digitally signed by the LRA (KEP) employee. An SMS is automatically sent to the subscriber's mobile phone informing that physical identification has been successfully completed.
- The Attestation of Identification is stored in the data base. In the APED application, the subscriber's Qualified Certificate management screen, indicates that the LRA office (KEP) has completed the identification and also shows the unique identification number.
- In case of failure of the identification, the employee records the reason for the rejection. The Subscriber receives an SMS that refers him to the APED application to be informed of the reason for rejection

ii. Remote Identification (according to no. 27499/2021 Decision of the Minister of State, article 3, par. 2)

- The LRA officer is authenticated in the APED portal using the credentials available through the General Secretariat of Information Systems and Digital Governance of the Ministry of Digital Governance (TaxisNet)
- The LRA officer carries out the remote identification.
- The application verifies through interoperability, as mentioned above in physical identification, the validity of the identification document.
- Once the identification is successfully completed, an Attestation of Identification is created on which the advanced or qualified electronic seal of the remote identification service provider or the qualified electronic signature of the employee who performed the remote identification is placed. An SMS is automatically sent to the Subscriber's mobile phone informing that the identification has been successfully completed
- The Attestation of Identification is stored in the APED database. A copy of the identification document and the video of the identification are stored in the database of the remote identification service provider. In the APED application, on the Subscriber's certificate management screen, it is displayed that the identification has been completed by an Authorized Office, along with the unique identification number.
- In case of failure of the identification, the LRA officer records the reason for the rejection. The Subscriber receives an SMS that refers him to the APED application to be informed of the reason for rejection

- The request is approved by the Registration Authority.
  - The RA officer navigates to the "Requests for Issuance of Qualified Certificates" screen and selects the request.
  - Checks the details of the application on the portal as well as the application - Declaration of gov.gr. Once he finds that everything is correct, he approves the request.
    - If the RA officer detects an irregularity, he rejects the request and the subscriber is informed by SMS. In the portal, the subscriber sees the rejection reason, and is informed of the corrective actions to be taken in order to resubmit the request.
  - The subscriber is informed by SMS on his mobile phone that the request has been approved. The message contains the eight-digit issuance/revocation code.
- Following the instructions, the subscriber proceeds to issue the qualified certificate.

The Citizen's application remains active and pending, for a period of ninety (90) days from its submission, so that the applicant of the qualified certificate can proceed with the identification before an LRA officer (physical identification) or by the method of remote identification, within the above-mentioned period.

After the expiry of the above-mentioned deadline, that is, without the applicant proceeding with the identification, in accordance with the above, this application is deleted without having any legal effect.

Throughout the process for the issuance of the Qualified Certificate, from the submission of the application to its approval by the CA, it is checked ex officio whether the applicant is alive, through interoperability with the Civil Registry. In case it appears that the applicant is not alive during the submission of the application, the procedure for issuing a qualified certificate is stopped and a relevant message appears on the applicant's screen. The same happens during the installation of the qualified certificate in the QSCD. In any case, the LRA officer who carries out the identification of the applicant for the issuance (and/or revocation) of the approved certificate, after checking the validity of the applicant's identification document, considers the result of the check through interoperability with the Civil Registry, regarding possible indication of death of the applicant. In addition, RA reserves the right to cancel the approved certificate in the event that, through interoperability with the Civil Registry, there is evidence of the death of the End User of the approved certificate (Subscriber). If death indication of the applicant/Subscriber has been falsely obtained, the applicant/Subscriber contacts the Civil Registry for the appropriate correction.

3.2.3 Non-Verified Subscriber information

Not applicable.

3.3 Identification and Authentication for Re-keying Requests

Rekeying is only supported for expired or revoked certificates. The identification process is described in §3.2.2.

3.3.1 Identification and authentication for routine re-key

Not applicable.

3.3.2 Identification and Authentication for Re-Keying after revocation

Key Regeneration after revocation is not possible if:

- The revocation occurred because the Certificates were issued to a person other than the one named as the Certificate Subject.
- The Certificates were issued without the consent of the person named as their Subject, or of the natural person authorized for this purpose.
- The person approving the Subscriber's Online Enrollment or Certificate Application discovers or has reason to believe that some essential information in the Online Enrollment or Certificate Application is false.

Under the above conditions, Subscriber Certificates, which have been revoked or expired, may be replaced (key pairs regenerated), in accordance with §3.2.2.

3.4 Identification and Authentication for Revocation Request

For the revocation of Subscriber Certificates, procedures are followed, recorded in the Practice Statements of the issuing CAs, which confirm that the user requesting the revocation is indeed the subject of the Certificate or a person authorized for this purpose (par. 4.9.3). The recall service is available 7 days a week, 24 hours a day.
To verify the identity of a Subscriber's revocation request, one of the following acceptable procedures is followed on a case-by-case basis:

- Revocation with 8-digit code.
    - In this case, the subscriber himself revokes his certificate without the intervention / involvement of the Registration Authority.

- The subscriber connects to the APED portal and chooses to revoke his certificate. He must enter the unique eight-digit code that was generated when the issuance request was approved and sent to him via SMS on his mobile phone. By entering the code and submitting the request, the certificate is automatically cancelled.
- If the subscriber has not saved the eight-digit code, he can ask for a reminder. In this case, he enters his tax identification number and date of birth and if these details are verified, an SMS with the code is sent to the mobile phone number registered in the issuance of the certificate. If the mobile phone number has been changed, the registered mobile phone cannot be modified and the reminder code cannot be received.

- Revocation with application at gov.gr
  - This option is used if the subscriber does not have the eight-digit code and cannot be reminded because he has changed his mobile phone number.
  - The subscriber navigates to gov.gr, locates the revocation request - Declaration, is authenticated (two-factor authentication, using a certified mobile phone) and creates it. The new certified mobile phone number is entered in the application-Declaration, with the certification process available on the gov.gr website
  - The subscriber connects to the APED portal and chooses to proceed with the revocation by entering the unique verification identification number (code) of the application - Declaration that he created on gov.gr.
  - By submitting the request, the basic fields are automatically checked (TIN, first name, last name) and the request is routed to the Registration Authority. The application-Declaration of gov.gr is stored in the database.
  - The Registration Authority checks the request and proceeds to revoke the Qualified Certificate.
  - The subscriber is informed by SMS about the revocation.
- Revocation in the event of failure of the application:
  https://services.aped.gov.gr/apedcitizen/login/
  In case of failure of the above application, due to a sudden and unforeseen event, the Subscriber may submit a revocation request by issuing an application/ Declaration form of revocation of a qualified certificate from the Single Digital Portal of the Public Administration (gov.gr) and sending it via e-mail to the e-mail address aped@mindigital.gr or by traditional mail to the Ministry of Digital Governance/APED, 11 Frangoudi str and Al. Pantou, Postal Code 17671.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL

4.1 Certificate Issuance Application

4.1.1 Who Can Submit a Certificate Issuance Application

For the issuance of a Qualified Subscriber Certificate, the person who can submit a Certificate application is the natural person who is the Subject of the Certificate

4.1.2 Enrollment Process and Responsibilities

For the issuance of Subscriber Certificates, all Subscribers are subject to a registration and identity verification process, which is described in the Certification Practice Statements of the issuing CAs, and which at least consists of:

- Physical presence of the Subscriber himself, at a competent LRA Office or, where deemed necessary, at representatives of the Registration Authority or the Issuing CA.
- Written or electronic acceptance of the Certificate Terms and Conditions of Use.
- Completing and signing the Certificate Application by providing true and accurate information in accordance with the requirements of this policy.
- Presentation of the relevant validation documents.
- Creation or submission of a request to create a key pair according to §6.1 of the CP.
- Receiving their certificate.
- Sending of the public key by the Subscriber, to the issuing CA, according to §6.1.3 of the CP.
- The Subscriber's proof to the issuing CA, in accordance with §3.2.1 of the CP, that he is in possession of the private signing key corresponding to the public key he sent to the issuing CA.

4.2 Certificate Issuance Application Processing

4.2.1 Approval or Rejection of Application of Subscriber's Certificate Issuance

Upon submission of the necessary legalizing documents, an authorized employee of the LRA Office or, where deemed necessary, the Registration Authority or Issuing CA, confirms the identification information in accordance with §3.2.2 of the CP. With the successful completion of all the required identification procedures, RA will proceed with the approval of the request for the issuance of the Certificate. If the authentication is not successful, it will reject it accordingly.

Subscriber Certificates are created and issued after the approval by the RA of the application submitted by the Subscriber. In particular, after the Subscriber is informed that the request has been approved, he must log in to the qualified certificate management application and follow the procedure for issuing the Certificate, as described in the Practice Statement of the issuing CA.

APED rejects an application for a certificate if:

- the identification and verification of the identity of all required details of the Subscriber cannot be completed or
- the Subscriber is unable to submit the relevant documentation requested or
- the Subscriber fails to respond to notifications within the specified time

4.2.2 Approval or Rejection of Certificate Application of SubCA

APED as Primary (Root) Certification Authority (PCA-RCA) certifies Subordinate Certification Authorities and signs the corresponding SubCA Certificates in accordance with the provisions of §1.3.1 of the CP

4.2.3 Time to Process Certificate Applications

CAs and RAs begin processing Certificate applications within a reasonable time of receipt. There is no specific provision regarding the time to complete the processing of applications, unless otherwise stated in the relevant General Terms and Conditions of Certificate Use or the Practice Statement of the issuing CA. Certificate applications remain valid for up to one month or until rejected.

4.3 Certificate Issuance

4.3.1 Issuing CA Actions during Certificate Issuance

The Certificate is created and issued by the Subscriber within the QSCD, after the certificate is forwarded by the LRA Office and approved by the RA. The Subscriber Certificate is created based on the details of the Certificate Application provided that the Application has been approved by the RA. For the approval of the Application, the submission of

identification documents by the Subscriber, specified in the Application Form for the issuance of a Certificate, is required.

The Subscriber must issue the Qualified Electronic Signature Certificate within fifteen (15) days of the approval of his application by the Registration Authority. After this period his application is canceled and he has to submit a new application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Issuing CAs that issue Certificates to Subscribers notify Subscribers, either directly or through an RA, that the certificate request has been approved, in order to proceed with its issuance process.

Certificates are made available to Subscribers from the Certificate Management Application (website), as defined in the CPS of the issuing CA.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificate usage or failure of the Subscriber to object to the Certificate or its content (in particular: Name, Surname, start date/ end date) within 24 hours from issuance, constitute Certificate acceptance by the subscriber

4.4.2 Publication of the Certificate by the CA

APED publishes its Certificate as well as the Certificates of the SubCAs that it issues according to the following Table 4.

Table 4: Publication Requirements

Certificate Form	Publication Requirements
APED Certificate	Available to Relying Parties online, through the APED repository, and as part of the Certificate Chain, which is embedded in the Subscriber Certificate.
SubCA Certificate	Available to Relying Parties online, through APED repositories and issuing CAs, and as part of the Certificate Chain, which is embedded in the Subscriber Certificate.

Issuing CAs publish the Certificates they issue in a publicly accessible online repository

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Issuing CAs may notify the RA of the issuance of Certificates which issuing CAs approve

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The use of the Private Key corresponding to the Public Key included in the Certificate will only be permitted if the Subscriber has agreed to the General Terms and Conditions and has accepted the Certificate. The Certificate will be used in accordance with the General Terms and Conditions, the terms of this CP and the applicable Certification Practice Statement of the issuing CA. In addition, the use of the Certificate must comply with the extensions of the KeyUsage field of the Certificate.

Subscribers are required to protect their private keys from unauthorized use and to discontinue their use upon expiration or revocation of the Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the General Terms and Conditions of APED as a condition of relying on the Certificate. Reliance on a Certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate for any given purpose, determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS and that the certificate is being used in accordance with the KeyUsage field extensions included in the certificate.
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to rely on a Certificate and perform signature verification.

APED and issuing CAs are not responsible for evaluating the appropriateness of use of the Certificates.

4.6 Certificate Renewal

Not applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Subscriber rekeying can be performed after the existing certificate is revoked or after its expiration

Table 6 below lists the requirements of APED for rekeying.

Table 6: Requirements of rekeying

Certificate Form	Απαιτήσεις Ανανέωσης
Subscriber Certificate	An essential condition for accepting the rekeying of a Subscriber Certificate is the verification of information performed by the issuing CA to confirm that the Subscriber's identity is still valid. This process is done in order to confirm that the person seeking to issue a Subscriber Certificate is in fact the Subscriber of the Certificate as referred to in §3.2.2 of the CP.
Certificates of SubCAs and APED	Re-generation of CA keys is done under strict control measures, in special Key Generation Ceremonies according to §6.1.1 of the Certificate Policy.

4.7.2 Who May Request Certification of a New Public Key

Only the Subscriber may request Certificate re-keying.

4.7.3 Processing Certificate Re-Keying Requests

Re-keying procedures ensure that the Subscriber seeking to re-key a Subscriber Certificate is in fact the Subscriber of the Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with §4.3.2 of the CP

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with §4.4.1 of the CP

4.7.6 Publication of the Re-Keyed Certificate by the CA

Issuing CAs publish re-keyed certificates in an information space accessible to the public, in accordance with §4.4.2 of the CP

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification from Issuing CAs of the issuance of Certificates that RAs approve.

4.8 Certificate Modification

Certificate Conversion is not provided. When one or more of the elements of the Certificate are changed, then a new Certificate is issued, according to the initial registration procedures described in §4.1 of the CP

4.9 Certificate Revocation

4.9.1 Circumstances for Revocation

4.9.1.1 Circumstances for Revocation of Subscriber Certificate

Subscriber Certificate is revoked if:

1. It is requested by the owner of the Qualified Certificate.
2. It is detected by the Hellenic Telecommunications and Post Commission (EETT) that the approved certificate contains false or inaccurate information regarding the requirements of Regulation (EU) 910/2014.
3. The issuance was based on false or inaccurate information.
4. The Trust Service Provider terminates business, unless, before the date of cessation of business, another qualified Trust Service Provider assumes the continued operation of the part of the service required.
5. The owner of the qualified certificate is a natural person and loses legal capacity, is declared in invalidity or in case of death.
6. Final court decision orders the revocation, after notification of the relevant decision to the Trust Service Provider.
7. The contract between the trust service provider and the holder of the approved certificate results in a relevant obligation or right of one of the contracting parties.
8. There are serious indications that the electronic signature creation data of the owner of the qualified certificate has become known or is being used by third parties.
9. The electronic signature creation data of the trust service provider has become known to third parties.
10. Any information included in the qualified certificate is modified.

The General Terms and Conditions of issuing CAs require Subscribers to immediately notify the issuing CA if they know or suspect their private key has been compromised in accordance with the procedures in §4.9.3 of the CP

4.9.1.2 Circumstances for Revocation of Certificates issued by APED

APED revokes certificates it issues for the SubCAs, if:

- It Discovers or has reason to believe that there has been an exposure of the SubCA private key.
- There is a relevant documented request from EETT.
- It discovers or has reason to believe that the SubCA Certificate has been issued in a manner that is not actually in accordance with the procedures required by this CP, that the Certificate of the SubCA was issued for an organization other than the one named as the Subject of the SubCA Certificate or without its approval.
- Determine that the conditions of this CP are not met or there is a waiver of an essential condition for the Issuance of a SubCA Certificate.
- APED ceases to function as CA.

4.9.2 Who Can Request Revocation

4.9.2.1 Who Can Request Revocation of Subscriber's Certificate

APED or the issuing CA is obliged to revoke any Subscriber Certificate it has issued, in accordance with the provisions of §4.9.1.1 of the CP.
Subscribers may request revocation of their own Certificates.
With the use of the Digital Certificate Management Application, APED performs a periodic check of users whose approved certificates are valid in order to confirm that they are alive, using the service of indication of life/death from the Citizen Registry. In case of detection of death indication of the user of the approved certificate, the application automatically revokes the certificate.

4.9.2.2 Who Can Request Revocation of SubCA Certificate

APED, SubCA and EETT have the right to request the revocation of a SubCA certificate issued for the latter.

4.9.3 Procedure for Revocation Request

A Subscriber wishing to revoke its Certificate must submit a revocation request in accordance with the documented procedures described in the issuing CA's Practice Statement. These procedures confirm that the person requesting the revocation of the Certificate is authorized for this purpose, in accordance with section §4.9.2 above. This request is forwarded to the responsible RA that has checked the Subscriber's Electronic Registration or Request for Certificates and which is competent to revoke it immediately.

4.9.4 Time within Which CA Must Process the Revocation Request

The relevant CAs take all reasonable steps to process revocation requests in a timely manner. In particular, applications for the revocation of Qualified Certificates are immediately processed by the RAs, which process the request within 24 hours.
Immediately after the revocation of the Certificate, the issuing CA informs the Subscriber of this fact, via e-mail to the address stated in the electronic application for the issuance of the certificate ("application at the APED portal") or text message (SMS). The issuing CA keeps relevant records proving that the relevant update has been carried out.

4.9.5 Revocation Checking Requirements for Relying Parties

Relying Parties should check the status of the Certificates they wish to rely on, using one of the certificate status checking mechanisms provided by the issuing CA.

In the case of the Certificate Revocation List, the Relying Party should check the status of the Certificate it wishes to rely on by referring to the most recent Certificate Revocation List (CRL) published by the CA or issuing CA that issued the Certificate.

For APED, the CRLs are listed in its storage area at: https://pki.aped.gov.gr/repository/gr/CRL/. In addition, a "CRL Reference Table" is published in the Repository at: https://pki.aped.gov.gr/repository/gr/CRL/, to allow Relying Parties to determine for each SubCA the exact storage location of the CRL. This location is also included in the certificate itself and is correct for the entire period of its validity.

Issuing CAs specify in their Practice Statement, the place of publication of the CRL they issue.

4.9.6 CRL Issuance Frequency

APED and issuing CAs provide uninterrupted Certificate revocation services. APED publishes CRL containing the Certificates that have been revoked by it and simultaneously offers Certificate status checking services.

CRLs for Subscriber Certificates issued by issuing CAs are published daily. The CRLs for certificates of issuing CAs issued by APED are published every year as well as every time a Certificate is revoked.

Information about the revocation status is made available even after the certificate's validity period, through the OCSP protocol.
Certificates may be removed from the CRLs after their expiration.

4.9.7 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is done automatically.

4.9.8 On-Line Revocation/Status Checking Availability

Certificate status information from issuing CAs may also be available through the use of the Online Certificate Status Protocol (OCSP).
When issuing CAs use the Online Certificate Status Protocol, they publish the addresses for OCSP Responders in their Certification Practice Statement, as well as the OCSP Certificate profile in accordance with the requirements of §7.3 of the CP. This information is also included in the certificates themselves and is correct for the entire duration of their validity.

4.9.9 On-Line Revocation Checking Requirements

Any Relying Party may check the status of a Certificate it wishes to rely on, using the method specified in §4.9.8.

4.9.10 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.11 Special Requirements regarding Key Compromise

In addition to the procedures described in §4.9.6 - 4.9.10 of the CP, APED makes every reasonable effort to inform the potentially Relying Parties with a relevant announcement at the online addresses https://pki.aped.gov.gr and https://www.aped.gov.gr or in other publicly accessible media, in the event that it discovers, or has reason to believe, that there has been an Exposure to Risk of the private key of an issuing CA, while at the same time it also informs EETT.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of the Certificates is available through the CRLs located on the websites of the issuing CAs at a web site - URL specified in the CPS of each issuing CA and OCSP responders.

4.10.2 Service Availability

Certificate Status Services are available 24 hours a day, 7 days a week, with a minimum total availability of 99% per year with planned outages not exceeding 0.4% per year

4.11 End of Subscription

Subscribers may terminate the use of the Certificates they hold either by letting their Certificate expire without re-keying that Certificate or by revoking their Certificate before it expires without replacing it

5. Physical, Management and Operational Protection and Security Measures

APED has implemented high security standards that correspond to this CP. APED's PKI is hosted in the infrastructure of a Qualified Trust Service Provider in which all the required physical protection and security measures are applied as described in this section, and in accordance with the Security Policy that has been prepared

5.1 Physical Controls

5.1.1 Site Location and Construction

The trust services of APED CAs are carried out within a physically protected environment which is designed to avert, prevent and detect any apparent or non-obvious access attempt, satisfying internationally recognized security standards, terms and conditions.
APED maintains Disaster Recovery facilities in respect of CA operations. APED's Disaster Recovery facilities are protected by multiple tiers of physical security.

5.1.2 Physical Access

In order to gain access to a higher tier of access, it is necessary to firstly gain access to a tier level. In particular, there are tiers of access that include:

- Public places.
- Tier at which the sensitive functional activity of CAs takes place.
- Storage space for Hardware Security Modules - HSM (Cryptographic Signing Units - CSU).

5.1.3 Power and Air Conditioning

Secure facilities of the infrastructures through which the trust services are provided, based on the provisions herein and the concluded contracts, are equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating / ventilation / air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

Reasonable precautions have been taken to minimize the impact of water exposure to systems

5.1.5 Fire Prevention and Protection

Reasonable precautions have been taken to prevent and extinguish fires or prevent other damaging exposure to flame or smoke. Fire prevention and protection measures have been designed to comply with national fire safety regulations.

5.1.6 Media Storage

All media containing software and production data, as well as audit, archive or backup data, are stored in secure storage facilities that have the necessary physical and logical access control measures. These measures are designed to limit access only to authorized personnel and to protect the storage media against any destruction (eg, water, fire and/or electromagnetic destruction)

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.
Remaining non-useful materials are destroyed

5.1.8 Off-Site Backup

Backup copies of key systems data, audit trail data, and other classified information are created at regular intervals. Backup copies are stored outside the main installation area with suitable means of protection.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees that have access to or control authentication or cryptographic operations that may materially affect:

- The validation of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or enrolment information
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository
- The handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- APED personnel,
- Cryptographic business operations personnel,
- Security personnel,
- System administration personnel,
- Designated engineering personnel, and
- Executives that are designated to manage infrastructural trustworthiness

5.2.2 Number of Persons Required per Task

Issuing CAs and RAs adopt and implement strict control measures to ensure segregation of duties for each area of responsibility and to ensure that more than one Trusted Person is required to perform high-level tasks.
High-level tasks, such as accessing and manipulating the CA's cryptographic hardware, require multiple Trusted Persons so that there is shared control over both physical and logical access to the hardware.
Persons who have physical access to cryptographic equipment do not hold "Private Shares" (§6.2.2), and vice versa.

5.2.3 Identification and Authentication for Each Role

CAs and RAs verify the identity and authorization of personnel who wish to be considered Trusted Persons before such personnel:

- obtain access devices and be granted access to the required facilities,
- obtain qualified certificates for accessing and performing specific responsibilities of Information Systems and CA or RA systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Segregation of Duties include but are not limited to:

- The verification of the data in the Certificate Applications.
- Accepting, rejecting or otherwise processing Certificate Applications, revocation requests or renewal requests or registration information.
- Issuance or revocation of Certificates for Administrators and personnel who have access to restricted access facilities.
- Creating, issuing, "loading" or destroying a CA certificate.
- Access to remote QSCD.

5.3 Personnel Controls

APED guarantees for the personnel who are going to acquire the status of a Trusted Person in terms of their formal qualifications and the experience required to perform the duties of the intended position in an adequate and satisfactory manner. For personnel holding Positions of Trust, background checks are repeated at least every five (5) years.

5.3.1 Qualifications, Experience, and Clearance Requirements

APED employees with the role of a Trusted Person have the obligation to maintain the secrecy of the confidential information of which they have become aware during the performance of their duties, and are not allowed to undertake initiatives or tasks incompatible with the trusted role assigned to them, or circumventing the principle of administration impartiality.
Issuing CAs document in detail the personnel and security audit policies they follow, compliance with which is part of the independent audit described in section §8 of the Certificate Policy.

5.3.2 Background Check Procedures

APED guarantees its employees are suitable for the execution of this CP and ensures the implementation of the civil service code and the relevant provisions, as they apply, in particular of the Disciplinary Law.
Before assigning the duties of a Role of Trusted Person, APED conducts an audit of the employee's file, in order to establish any disciplinary or other conviction. The above assignment is subject to the condition that there is no disciplinary or other conviction of the employee who will assume the trusted role.
The use of information disclosed during a background check to take relevant action is subject to applicable privacy and confidentiality laws.

5.3.3 Train Requirements

APED provides its staff with training deemed necessary for the performance of their work duties in an adequate and satisfactory manner. The training implemented by APED includes the following:

- the basic concepts of PKI,
- job responsibilities,
- the security and operation policy and procedures of the APED,
- the use and operation of the equipment and software that has been developed,
- incident reporting and response, Risk Exposure, disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

APED and issuing CAs ensure continuous training and updating of current developments to their staff to the extent and frequency necessary to ensure the maintenance of the required level of knowledge proficiency. Information regarding security issues is also provided on a continuous basis.

5.3.5 Sanctions for Unauthorized Actions

In the case of unauthorized actions or other violations of APED policies and procedures, appropriate disciplinary measures are taken. Such disciplinary measures are determined according to the frequency and severity of the unauthorized actions and are in accordance with the civil service code, as applicable.

5.3.6 Independent Contractor Requirements

Trusted Positions are also filled by independent contractors who are subject to the same operational and safety criteria that apply to APED employees. Access to the secure facilities hosted by APED is permitted only to Trusted Persons, who are either employees of APED, or belong to an independent contractor. Issuing CAs and RAs may allow independent contractors to act as Trusted Persons only to the extent necessary to serve clearly defined delegation relationships and only under strict conditions. A relevant contract is needed, that has been checked by a Conformity Assessment Body and has been previously approved by EETT.

5.3.7 Documentation Supplied to Personnel

Employees who undertake the implementation of PKI trust services based on the provisions herein, receive full knowledge of this Policy and the applicable Practice Statement, as well as the required training and other documentation, for the proper performance of their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

APED ensures, where required, the recording of important life cycle management incidents of keys and Certificates of APED and SubCAs, including:

- Generating, backing up, storing, retrieving, archiving and destroying keys and
- Lifecycle management incidents of encryption devices.

Issuing CAs ensure, where required, the recording of important life cycle management incidents of Subscriber Certificates, including:

- Registration Information,
- Successful or unsuccessful processing of Online Entries or Applications for Certificates, revocation and recovery, and
- Production and issuance of Certificates and CRL.

The APED and issuing CAs shall ensure, where required, the recording of the following security-related incidents concerning them, including:

- Successful or unsuccessful attempts to access the PKI system.
- PKI and security system activities.
- Access of highly secure files or registers that are available for reading, writing or deletion.
- Changes in the security level.
- System jams, equipment failures or other anomalies.
- Activity of the protection system (firewall) and router.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Type of entry.

The Registration Authorities and/or LRAs record the registration details including:

- The type of supporting documents for the identification of the Subscriber.
- The identification document number.
- The content of the identification document (surname, first name, issuing authority, etc.), if there is interoperability with the corresponding electronic register of the document.
- For remote identification, a copy of the identification document and the video of the conference
- Surname and first name of the person carrying out the identification
- Method used to confirm identification documents, if applicable.

5.4.2 Frequency of Processing Log

Logs are reviewed on a regular basis for significant security and operational incidents. In addition, APED and respective issuing CAs ensure the review of logs for suspicious or unusual activity based on the warning messages generated when there are irregularities or problems within the system of this PKI.

5.4.3 Retention Period for Audit Log

Log files are kept on-site for at least two (2) months after processing, and are then archived in accordance with §5.5.2 of the CP.

5.4.4 Protection of Audit Log

Electronic and manual log files are protected from unauthorized reading, modification, deletion or other tampering by using physical and logical access control measures.

5.4.5 Audit Log Backup Procedures

Incremental backups of the log files are produced every hour. An advanced electronic signature and time stamp is placed on the files. Full backups are produced on a weekly basis.

5.4.6 Audit Collection System

Automated audit data is generated and recorded at the application, network and operating system level

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event, unless such notice is compulsory according to the law.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons who have a legal right of access.

5.4.8 Vulnerability Assessments

Events that occur during the audit process are logged so that system vulnerabilities can be tracked.
System vulnerability assessments are conducted, audited and reviewed. The annual Vulnerability Assessment will be a point of reference in terms of the annual audit of APED.

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to log control records for security purposes specified in §5.4 of the CP, APED ensures that records are maintained that include documentation of the following:

- Compliance with the CP.
- Actions and information that are essential for the issuance of each Certificate as well as for the creation, issuance, revocation, expiration and re-keying of all SubCA Certificates issued.

Certificate lifecycle records maintained by issuing CAs include:

- The obligations arising from the General Terms and Conditions of Use.
- Any change that has occurred in the General Terms and Conditions of Use.
- The identity of the Subscriber named in each Certificate.
- The identity of the person requesting the revocation or recovery of a Certificate.
- Other facts stated in the Certificate.
- Certain material information related to the issuance of Certificates, including, but not limited to, information regarding the successful completion of the Conformity Audit in accordance with §8 of the CP.

The records kept by the issuing CAs regarding the identity of the Subscribers include the following in electronic form:

- Application – Declaration form on gov.gr, which contains an identity card or passport number
- APED application
- Attestation of Physical or Remote Identification of the subscriber, digitally signed with the use of a qualified electronic signature by the employee who carried out the identification (physical or remote) or advanced or qualified electronic seal of the remote identification service provider

Records may be kept electronically or in hard copy, provided they are accurately classified, stored, maintained and reproduced as a whole.

5.5.2 Retention Period for Archive

Physical or digital records of certificate applications, registration information, and requests or applications for revocation shall be retained for at least seven (7) years after the expiration of any certificate based on such records.

In the event of termination of the operation of the CA, the logs and files of the APED are preserved and they are accessible until the above-mentioned retention period in accordance with section §5.8.

5.5.3 Protection of Archive

APED ensures the protection of logs recorded in accordance with §5.5.1 of the CP, in such a way that only authorized persons are allowed to have access to them. Electronically archived data is protected against unauthorized reading, modification, deletion or other tampering by implementing appropriate physical and logical access control measures. The media holding the archived data, as well as the required applications for the processing of this data, are kept in order to ensure their accessibility, for the period of time specified in §5.5.2 of the CP.
Similar measures are applied by issuing CAs to protect the files they keep.

5.5.4 Archive Backup Procedures

APED creates on a daily basis, where required, backup copies of the data contained in the issued Certificates, together with the back-up of the entire Database, with the use of incremental backups, while producing full backups on a weekly basis.
Issuing CAs apply measures of a corresponding level of security.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. Such time information is not cryptographic-based.

5.5.6 Procedures to Obtain and Verify Archive Information

See CP §5.5.3.

5.6 Key Changeover

CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in §6.3.2 of the CP.

Prior to the expiration of the CA's Certificate for a parent CA, key replacement procedures are carried out to facilitate a smooth transition of entities within the parent CA hierarchy from the old key pair to the new key pair. The CA key replacement process assumes that:

- The Parent CA stops issuing new Certificates of the SubCAs no later than 60 days before the point in time (hereinafter "Issuance Stop Date") where the remaining lifetime of the key pair of the Parent CA is equal to the Period Validity of the approved Certificate for the specific type of Certificates issued by the SubCAs in the hierarchy of the Parent CA.
- Certificates, upon acceptance of an SubCA (or End-User Subscriber) Certificate Request received after the "Issuance Stop Date", will be signed with the CA's new key pair.

The parent CA continues to issue CRLs signed with the parent CA's original private key until the expiration date of the last Certificate issued using that original parent key pair.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backup copies of the following CA information are stored in a warehouse off-site and made available in the event of a Compromise or destruction: Certificate Application data, audit data and database records for all issued Certificates. Backup copies of the CA's private keys are created and maintained in accordance with this CPS.

APED informs, without undue delay and, in any case, within 24 hours after becoming aware of the matter, the supervisory body Hellenic Telecommunications and Post Commission (EETT), the General Directorate of Cyber Security of the Ministry of Digital Governance and, as the case may be, the National Computer Emergency Response Team (National CERT) and the DPO of the Ministry of Digital Governance, for any breach of security or loss of integrity that has a significant impact on the provided trust service or the related personal data (event impact level 3 or greater, according to the classification defined in the Regulation on the Provision of Trust Services of EETT, article 5).

When the security breach or loss of integrity is likely to adversely affect a natural or legal person to whom the trust service has been provided, APED shall also, without undue delay, inform the natural or legal person of the security breach or loss of integrity.

5.7.2 Corruption of Computing Resources, Software and/or Data

In the event of corruption of computing resources, software and/or data incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation and incident response. If necessary, disaster recovery or key compromise procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

In the event of the alleged or actual Compromise of the private key of the APED or issuing CAs, special measures are applied to deal with the Compromise by executives of the management body of the Public Key Infrastructure. These executives assess the situation, develop an action plan and execute this plan with the approval of the APED.

If CA Certificate revocation is required, the following measures are taken:

- The Hellenic Telecommunications & Posts Commission (EETT) is notified.
- EETT can withdraw the Certificate from the Trust List of supervised/accredited Trust Service Providers – TSL.
- The revocation status of the SubCA Certificate is communicated to Subscribers and Relying Parties through the Storage Area of APED and the issuing CA in accordance with §4.9.5 of the CP.
- A reasonable effort is made to provide additional information regarding the revocation to all participants who may be affected.
- The CA will generate a new key pair and new CA certificate according to §5.6 of the CP, except in the case where the provision of certification services is interrupted according to §5.8 of the CP

5.7.4 Business Continuity Capabilities after a Disaster

To ensure the continuation of business operations after a disaster, backup files are created for the critical components of the APED and the issuing CAs for the PKI, both hardware and software. In addition, copies of the private keys of the APED and issuing CAs are taken for disaster recovery purposes. Measures are also developed to implement a disaster recovery plan. This plan includes the existence of a disaster recovery area to minimize the consequences of any natural or other disaster. The above strategy is regularly reviewed, tested and updated to be operational in the event of a disaster. These measures are able to achieve restoration of information systems and basic business operations. Finally, copies of the important information of APED and issuing CAs are kept in another location. Such information includes, in particular, system and application logs, control elements, as well as the database files for all Certificates issued.

5.8 CA or RA Termination

In the event that it is necessary to terminate the provision of the trust services of a CA, the said CA is obliged by any appropriate means to inform those directly affected, the Subscribers, Relying Parties, etc., of the termination of the provision of the of trust services before it occurs, with a relevant notification to its e-mail address. For the termination of APED's trust services, the relevant announcement is published at http://www.aped.gov.gr

In the event of the termination of the provision of trust services by APED or an issuing CA in accordance with the above, a Termination Plan is developed by the CA that complies with the current Regulation on the Provision of Trust Services and point (i) of paragraph 2 of article 24 of EU Regulation 910/2014 (eIDAS), and may include, depending on the case, the following:

- notification of the parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,

- revocation of the Certificate issued to the CA by APED,
- preservation of the records and archives of the CA for the periods of time required by this CPS,
- continuous provision of Subscriber support services,
- continuous provision of revocation services, such as the issuance of CRLs or the maintenance of online Certificate status checking services,
- revocation of Subscriber Certificates and subordinate CAs which have not expired or been revoked, if necessary,
- disposition of the CA's private key, including the backup key and the hardware tokens containing such private key;
- necessary arrangements for the transition of the CA's services to the successor CA, where possible;
- notification of The Hellenic Telecommunications & Posts Commission (EETT)
- transfer of the obligations to a reliable party regarding the maintenance of the records and archives of the CA for the period of time required by this CPS and the eIDAS Regulation, as well as the continuous provision of revocation services, such as the issuance of CRLs or the support of network certificate status checking services
- submission of the archives and records of the APED CA to another contracting Trust Service Provider for Qualified Certificates for the time periods required by law.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by trained and trusted individuals using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. CA keys are generated in Key Generation Ceremonies, which conform to the requirements contained in the recorded confidentiality policies and procedures implemented by APED.

The generation of signature key pairs for both the RA manager and Subscribers is carried out using a Qualified Signature Creation Device (QSCD), which complies with the requirements of EU Regulation 910/2014 (eIDAS). In particular, during the process of Electronic Registration or Application for Certificates:

- The Subscriber uses a specific QSCD model, as stated in the instructions posted by APED at www.aped.gov.gr
- The Subscriber creates a public-private signature key pair within the QSCD through the APED Qualified Certificate Management Application, following the relevant instructions at www.aped.gov.gr. The application uses the necessary middleware to communicate with the driver of the specific QSCD and complete the process in an automatic way. The private signing key remains in the QSCD.
- The public key with the Subscriber's details is sent to the Certification Authority to be signed.

The production, storage and further use of the keys of the remote Qualified Digital Certificates is carried out or controlled by APED using exclusively devices certified in accordance with the requirements of Article 30.3 of the EU Regulation 910/2014 (eIDAS), which are included in the list of qualified devices maintained by the European Commission in compliance with articles 30, 31 and 39 of the eIDAS Regulation.

6.1.2 Private Key Delivery

Subscriber key pairs are generated on the QSCD by the Subscriber, so private key delivery to the Subscriber is not applicable.

When the key pairs are generated in a remote QSCD by the Subscriber, the private key is generated and stored within the remote QSCD.

6.1.3 Public Key Delivery to Certificate Issuer

Subscribers submit electronically their public key to the issuing CA that will provide the trust services, using a PKCS#10 Certificate Signing Request (CSR) or other digitally signed format, through a secure SSL connection (Secure Socket Layer Connection).

6.1.4 CA Public Key Delivery to Relying Parties

APED makes the subCA Certificates available to Subscribers and Relying Parties through the repository (https://pki.aped.gov.gr/repository).
Issuing CAs provide their own full certificate chain to the Subscriber upon Certificate issuance.

6.1.5 Key Size

Key pairs shall be of sufficient length to prevent third parties from determining the key pair's private key using cryptanalysis during the expected lifetime of those keys. The CA standard for minimum key size is to use a key pair of at least 2048-bit RSA strength for the CA and Subscriber certificates.
All CA and Subscriber certificates use the SHA-256 hash algorithm for digital signatures.

6.1.6 Public Key Parameters Generation and Quality Checking

The quality of public keys is guaranteed by using secure random number generation mechanisms that are integrated in the QSCD

6.1.7 Key Usage Purposes

See CP §7.1.2.1.

6.2 Private Key Protection

APED ensures the application of a combination of physical, logical and procedural measures which guarantee the security of the private keys of its CAs. Physical access control measures are described in §5.1.2 of the CP. Issuing CAs apply security measures of a similar level to those applied by APED.
Subscribers are required to take reasonable precautions to prevent the loss, disclosure, alteration or unauthorized use of their private keys.

6.2.1 Cryptographic Module Standards and Controls

For the generation and storage of APED and issuing CA private keys, hardware cryptographic modules compliant to eIDAS Regulation are used (QSCD). Subscriber private keys are generated on QSCD compliant to eIDAS Regulation requirements.
APED monitors QSCD certification status until the end of the validity period of the certificate associated with the relevant QSCD. In case of a modification of the certification status of the QSCD, APED will stop issuing certificates on these devices.

6.2.2 Private Key (m out of n) Multi-Person Control

Multi-Person Verification is intended to protect the activation data required to activate CA private keys, which are held by Certification Authorities. APED uses “Secret Sharing” to split private keys or the activation data needed to make use of a private key into separate parts called “Secret Shares”, which are held by individuals called “Shareholders”. A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a private key.

The threshold number of shares needed to sign a CA certificate is three (3). It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.
No Multi-Person control is applied to Subscriber Private keys.

6.2.3 Private Key Escrow

CA or subscriber’s private keys are not escrowed by APED or issuing CAs

6.2.4 Private Key Backup

APED creates back-up copies of CA private keys and Subscriber private keys generated by and stored in a remote QSCD, in case of recovery (regular or emergency). These keys are stored in an encrypted form within cryptographic modules that meet the specifications of §6.2.1 of the CP. CA private keys are copied to backup cryptographic units according to

§6.2.5 of the CP. Subscriber's private keys stored in QSCD cannot be extracted or restored from the QSCD and are not backed up.

6.2.5 Private Key Archival

At the end of their validity period, the key pair of the APED and issuing CA is archived for a period of at least 5 years. The archived CA key pair is stored in a secure manner using hardware cryptographic modules that meet the specifications of §6.2.1 of the CP. Procedural controls prevent archived APED key pairs from being returned to production use. At the end of the archiving period, the archived APED private keys will be destroyed in a secure manner and in accordance with §6.2.10 of the CP.
APED and issuing CAs do not archive copies of Subscriber's private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

When it is necessary to transfer a backup copy of a CA key pair to another cryptographic unit, the transfer is done securely to prevent its loss, theft, alteration, unauthorized disclosure or unauthorized use. Private keys are in encrypted form during transfer.
When the Subscriber's key pairs are backed up to other cryptographic hardware units, they are transferred between the units in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

Private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating a Private Key

Subscribers who obtain Certificates in accordance with the CP and/or in cases where the issuing CA requires it, must follow the Certificate issuance instructions posted at www.aped.gov.gr. At the same time, it is considered mandatory by the Subscribers:

- to use the QSCD PIN/Personal Identification Number (or the secret PUK/Personal Unblocking Key number in case of loss of the PIN), in accordance with §6.4.1 of the CP to verify their identity before activating their private key.
- to take appropriate measures for the physical protection of their space and workstation to prevent the use of the above as well as the corresponding private keys without their approval.

An online CA private key is activated by a certain number of Shareholders, as defined in section 6.2.2, by providing the activation data (which is stored on secure media). Once the private key is activated, it can remain active indefinitely until it is deactivated when the CA is taken offline. Likewise, a certain number of Shareholders must provide their activation data in order to activate the offline CA private key. Once the private key is activated, it remains active for only one connection.

6.2.9 Method of Deactivating a Private Key

CA private keys are deactivated by removing them from the reader.
Subscriber private keys can be disabled by removing the QSCD from the workstation or by disconnecting from the remote QSCD. In any case, Subscribers have an obligation to adequately protect their private keys in accordance with §6.4 of the CP.

6.2.10 Method of Destroying a Private Key

Where required, APED destroys CA and Subscriber private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. APED utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, key destruction activities are witnessed.
The Subscriber Private Keys of a Local QSCD can be destroyed by initializing or physically destroying or damaging the QSCD.

6.2.11 Cryptographic Module Rating

See §6.2.1 of the CP.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

APED CA and Subscriber Certificates are backed up and archived as part of routine backup procedures.
All the Subscriber Public Keys are kept in the database of APED and may be archived for at least seven (7) years after expiration of the Subscriber certificates.

6.3.2 Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Functional Period for the key pairs is the same as the Functional Period of the corresponding Certificates. Private keys can of course continue to be used for decryption and public keys for signature verification. The maximum Operational Periods of CA Certificates for Certificates issued from the entry into force of this CP and thereafter are listed in Table 7.
In addition, APED and issuing CAs stop issuing new Certificates in time before their Certificate expires, so as to ensure that no Certificates issued by APED or issuing CAs expire after their own Certificate expires.

Table 7: Certificate Operational Periods

Certificate	Operational Period
Primary (Root) Certification Authority (APED)	Up to 20 years
Issuing CA	Up to 10 years
Certificate	Up to 3 years

The CA and issuing CAs stop using the CA key pairs after their usage period ends. Subscribers cease using their key pairs after their usage periods expire. If an algorithm or corresponding key length does not provide sufficient security during the certificate's validity period, that certificate will be revoked and a new certificate request will be initiated. The applicability of cryptographic algorithms and parameters is continuously monitored by APED.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used (PIN) for the protection of the local QSCD containing the Subject's private keys are generated in accordance with the respective manual of the QSCD.
Default activation data must be changed immediately prior to the production of keys by Subscribers.
Activation data (user code, password and one-time password) for the protection of remote QSCD, containing the Subject's private keys, is generated according to QSCD compliance requirements to achieve exclusive control by the signatory with a high level of assurance , as defined in the eIDAS Regulation, Article 26, para. (c).

6.4.2 Activation Data Protection

Subscribers must take all necessary measures to safeguard and not disclose their private key activation data. They should remember activation codes (PIN, PUK, user code, password and one-time password) and do not share them with anyone else.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure or unauthorized use of such private keys.

6.4.3.2 Activation Data Destruction

Activation data for private keys are decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure or unauthorized use of the private keys protected by such activation data. After the record retention periods in section 5.5.2 lapse, APED destroys activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

All CA functions are performed using trustworthy systems

6.5.1 Computer Security Technical Requirements

All CA software and file systems are Trusted Systems secure from unauthorized access. General application users do not have accounts on production servers.
There is also a logical separation of the production network from the other departments so that access is allowed only through defined procedures.
Protection systems (firewalls) are used to protect the production network from internal and external intrusion, as well as to limit the nature and origin of activities that could access these systems.
Finally, the use of passwords is required, which will be changed on a periodic basis, with a certain number of characters and a combination of alphanumeric and special characters.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

New versions of software are developed and implemented in accordance to change management procedure.
New or updated software, when first loaded provides a method to verify that the software on the system originated from trust source, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

APED ensures compliance with the terms and conditions of this CP by the systems of APED and issuing CAs. APED periodically verifies the integrity of the systems of APED and the issuing CAs.

6.6.3 Life Cycle Security Controls

APED policies and assets are reviewed at planned intervals, or when significant changes occur to ensure their continuing suitability, adequacy and effectiveness. The configurations of systems are checked at least annually for changes that violate the APED security policies
APED has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

6.7 Network Security Controls

All CA trust services are provided using secure networks in accordance with the applicable Security Policy to prevent unauthorized access or other malicious activity.
Sharing of confidential information is also protected using encryption and qualified signatures.

6.8 Time-Stamping

Log files, Certificates, CRLs and other revocation database records include date and time information

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

This paragraph defines the specifications of the Profile and the content Certificates of APED and issuing CAs issued in accordance with this CP.

APED Certificates comply with (a) ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, August 2005 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 ("RFC5280") [X.509 Internet Public Key Infrastructure Certificate Profile and CRL]. Also, the basic fields of the Certificates are in compliance with EU Regulation 910/2014. This means that the Certificates following the CP include:

- Signature verification data (subject public key).
- Start and end of the validity period (valid from - valid to).
- The identification code of the certificate (serial number).
- The Qualified Electronic Signature of the Trust Service Provider issuing the certificate.

At a minimum, APED and issuing CA X.509 Certificates include the basic X.509 Version 3 fields and the proposed values or value restrictions listed in the following table

Table 8: Basic profile fields of Certificate

Field	Value or Value Restriction
Version	See CP §7.1.1
Serial Number	Unique value for each Subject Distinguished Name (Subject DN)
Signature Algorithm	The algorithm used for the signing of the Certificate (see §7.1.3 of CP)
Issuer DN	See §7.1.4 of CP
Valid From	Based on Universal Coordinate Time. Encoding according to RFC 5280.
Valid To	Based on Universal Coordinate Time. Encoding according to RFC 5280. The validity period will be determined in accordance with the limitations set forth in §6.3.2 of the CP.
Subject DN	See §7.1.4 of CP
Subject Public Key	Encoded according to RFC 5280 using algorithms specified in §7.1.3 of the CP and with key lengths specified in §6.1.5 of the CP
Key Size	4096

7.1.1 Version Number(s)

All Certificates of issuing CAs and subscribers are X.509 version 3 Certificates and their version field has the value of V3, according to RFC 5280.

7.1.2 Certificate Extensions

Extensions required according to §7.1.2.1 - §7.1.2.9 of the CP are indicated in the X.509 Certificates Version 3.

7.1.2.1 Key Usage

The data contained in the KeyUsage extension for the X.509 Version 3 Certificates of APED, issuing CAs and Subscribers are in accordance with RFC 5280: InternetX.509 Public Key Infrastructure Certificate and CRL Profile. The criticality field of the KeyUsage extension generally takes the value True.

TAble 9: Settings for the Key Usage Extension

	CAs
Criticality	**TRUE**
1 keyCertSign	set

2	CRLSign	set
3	Off-line CRL	set

		Subscriber Certificate for Signature – Authentication
Criticality		**TRUE**
1	Digital Signature	set
2	Non-Repudiation	set

7.1.2.2 Certificate Policies extension

X.509 Version 3 Subscriber Certificates use the "Certificate Policies" extension where the valid object identifier is listed, according to §7.1.5 of the CP, and the policy qualifiers are listed, according to §7.1.6 of the CP. The criticality field of this extension is set to FALSE.

7.1.2.3 Subject Alternative Names

The “Subject Altetnative Name” extension is supported for X.509 version 3 certificates according to RFC 5280. The criticality field of this extension is set to FALSE. In this extension and more specifically, in the same attribute of the RFC822 Name type, the e-mail address of the Certificate holder is optionally included.

7.1.2.4 Basic Constraints

The Basic Constraints extension in the X.509 Version 3 SubCA Certificates where the CA field is set to TRUE. In the Subscriber Certificates issued by issuing CAs the field of the “Basic Constraints” extension remains blank indicating that it is defined as EndEntity. The criticality field of the “Basic Constraints” extension is set to TRUE for Issuing CAs and subscriber Certificates.

Issuing CAs X.509 version 3 Certificates are issued by setting the “Maximum Path Length” field of the “Basic Constraints” extension the maximum number of CA certificates that can follow this Certificate in a certification path. Issuing CA Certificates have the value "0" in the “Maximum Path Length” field indicating that only one Subscriber Certificate can follow the certification path.

7.1.2.5 Extended Key Usage

The “Extended Key Usage” extension is used by issuing CAs for the Subscriber Certificates they issue (X.509 Version 3) in the following cases (Table 10).

Table 10: Settings for “Extended Key Usage” extension

		Πιστοποιητικό Ηλεκτρονικής Υπογραφής
Criticality		**FALSE**
1	ClientAuth	Set
2	Document Signing	Set
3	Secure email	Set

7.1.2.6 CRL Distribution Points

Subscriber Certificates include the CRL Distribution Points extension which points to the URL where a Relying Party can obtain a CRL to check the status of a Certificate. The criticality field in this extension is set to FALSE

7.1.2.7 Authority Key Identifier

The ability to use the Authority Key Identifier extension is provided for issuing CA Certificates and has a value of Root SKI, while for Subscriber Certificates it has the issuer's SKI.

7.1.2.8 Subject Key Identifier

The ability to use the Subject Key Identifier extension is provided for the self-signed CA Certificate, CA Issuer Certificates, and Subscriber Certificates. The keylidentifier generation method is calculated at least according to the methods described in RFC 5280 (more secure methods are not excluded).

7.1.3 Algorithm Object Identifiers

X.509 certificates of APED and issuing Cas are signed using sha256WithRSA Encryption according to RFC 3279.

7.1.4 Name Forms

APED and issuing CAs indicate the Distinctive Name of the Issuer and the Subject on their Certificates, in accordance with §3.1.1 of the CP.

7.1.5 Certificate Policy Object Identifier

The Subscribers' Certificates will include an identifier for the Certificate Policy they will follow, according to §1.2.1 of the CP. The APED subCA Certificates will include a Certificate Policy Identifier, i.e. 1.2.300.0.110001.2.1.1.

7.2 CRL Profile

The APED and issuing CAs issue CRLs that conform to RFC 3647. At a minimum, those CRLs include the key fields and contents specified in Table 11:

Table 11: Basic Fields of CRL Profile

Field	Value or Value Constraint
Version	See §7.2.1 of CP.
Signature Algorithm	Algorithm used to sign the CRL. CRLs of APED and issuing CAs are signed using sha256WithRSAEncryption according to RFC 3279
Issuer	The Agency that signs and issues the CRL. The CRL Issuer Name complies with the Issuer Distinguished Name specifications set out in §7.1.4 of the CP.
EffectiveDate	Issue Date of the CRL. The CRLs of APED and of issuing CAs are valid upon their issue.
NextUpdate	Date on which the next CRL will be issued. The frequency of issuance of CRLs is in accordance with the specifications of §4.9.6 of the CP.
RevokedCertificates	List of revoked Certificates, including the serial number of the revoked Certificate and revocation date

7.2.1 Version Number

APED and issuing Cas issue X.509 version 2 CRLS

7.3 OCSP Profile

Issuing CAs provide OCSP (On-line Certificate Status Protocol) services. OCSP Responders conform to the RFC 6960 standard.

At a minimum, OCSP Certificates include the key fields and contents specified in Table 12.

Table 12:

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version	See CP §7.1.1

Serial Number	Unique value for each Issuer Distinguished Name (Issuer DN)
Signature Algorithm	The algorithm used for the signing of the Certificate (see §7.1.3 of CP)
Issuer DN	Issuing CA
Validity Start	Based on Universal Coordinate Time. Encoding according to RFC 5280.
Validity End	Up to ten (10) years (equal to the operational lifetime of the issuing CA)
Subject DN	Like issuing CA with the difference of adding "OCSP Responder" to the end of the CommonName
Public Key Algorithm	Encoded according to RFC 5280 using algorithms specified in §7.1.3 of the CP and with key lengths specified in §6.1.5 of the CP.

7.3.1 Version Number

Issuing CAs that provide OCSP services, issue Version 1 Certificates, as specified in RFC 6960.

8. Compliance Audit and Other Assessments

APED is evaluated for the trust and key management services it provides, by an independent conformity assessment body in accordance with EU Regulation 910/2014 (eIDAS), the corresponding legislation and standards or whenever there is a significant change in the functions of the Trust Service.
In addition to compliance audits, APED is entitled to carry out other inspections and investigations to ensure the reliability of the Trust Services. APED is entitled to delegate the execution of these audits, inspections and investigations to a third-party auditing company.
APED is entitled to carry out a second round of checks on contractors who have entered into a relationship with APED to operate as Local Registration Authorities (LRAs).

8.1 Frequency of Assessment

APED Compliance Audits are conducted at least annually. Audits are conducted over unbroken sequences of audit periods with each period no longer than one-year duration.

8.2 Identity/Qualifications of Assessor

Compliance audits of APED's CA are performed by the following:

- Internal Auditors,
- The conformity assessment body which has been accredited according to regulation (EC) no. 765/2008 and the EN 319 403 standard as being capable to assess the compliance of Qualified Trust Service Providers and the Qualified Trust Services they provide,
- The Supervisory Body.

8.3 Assessor's Relationship to Assessed Entity

The auditor of the conformity assessment body shall be independent from APED and APED’s assessed systems.
The internal auditor shall not audit his/her own areas of responsibility.

8.4 Topics Covered by Assessment

Subject of the compliance audit is the information system, the security measures taken, the key management services and the control measures of the public key infrastructure, and in general the compliance of the audited Certification Authority with this Certificate Policy and with the applicable European Union and National Law about electronic signatures.

8.5 Actions taken as a Result of Deficiency

If, during the Compliance Audit, significant deficiencies or inadequacies are revealed, the required measures must be taken. APED will determine these measures following the auditor's recommendation. APED assesses the importance of the deficiencies and prioritizes the corresponding actions that must be taken at least within the time limit set by

the Supervisory Body or within a reasonable period of time. APED is in any case responsible for the development and implementation of the remedial action plan within a reasonable period of time.
When, during the EETT audit, there are indications that the personal data protection rules have been violated, the Supervisory Body informs the data protection authorities about the results of the compliance checks.

8.6 Communication of Results

The certificate(s) for the trust service(s), which are based on audit results of the conformity assessment body carried out in accordance with EU Regulation 910/2014 (eIDAS), the corresponding legislation and standards, may be published on the APED website. In addition, APED submits the relevant report for the assessment of compliance to the Supervisory Body within three (3) working days after receiving it.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Fees for issuing or renewing the Certificates are determined by APED's pricing policy, published at www.aped.gov.gr

9.1.2 Certificate Access Fees

APED and issuing CAs do not charge fees for the availability of a Certificate in storage or for otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

APED and issuing CAs do not charge fees for the availability of certificate revocation or status information as provided in §4.9.6 and 4.9.8 hereof or for otherwise making CRLs available to Relying Parties. APED and SubCAs do not allow access to Certificate revocation or status information in its storage space to third parties who provide products or services and make use of this information without its prior explicit consent.

9.1.4 Fees for Other Services

APED does not charge a fee for access to this CP. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation is subject to the provisions of Law 4305/31-10-2014 (Government Gazette 237 A')

9.1.5 Refund Policy

Not applicable.

9.2 Liability

The Greek State is liable for damage caused by acts or omissions of the APED bodies or the issuing CAs to any natural or legal person, due to non-compliance with the obligations provided for in this regulation, in accordance with article 105 of the Introductory Law of the Civil Code.
General Terms and Conditions for the use of Qualified Trust Services limit the liability of APED. Limitations of liability include the exclusion of indirect, special, incidental and consequential damages. In particular, for the responsibility of the Greek State due to actions or omissions of the bodies of APED, in terms of compliance with the provisions of the present, the following apply:
The Greek State is not responsible for any malfunction of APED services in cases of force majeure, such as, indicatively, earthquakes, floods, fires, etc., including cases of interruption of the electricity supply (black-out), problems in telecommunication networks and in general of all of 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 "Liability and burden of proof" of Regulation 910/2014 apply in this case, pursuant to paragraph 3 of the same article.

9.3 Confidentiality of Information

9.3.1 Scope of Confidential Information

In this case, the provisions for personal data protection, confidentiality of communications and any other relevant provision apply. In particular, the following files are considered confidential:

- CA records of applications, either approved or rejected.
- Certificate Application Files.
- Control files of APED and issuing CAs.
- Contingency prevention planning and disaster recovery plans.
- Security measures that control the operations of the equipment and software of APED and issuing CAs.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, revocation or other information related to the status of Certificates, web sites of APED and issuing CAs, as well as the information contained therein are not considered Confidential Information.

9.3.3 Responsibility to Protect Confidential Information

Participants in the PKI of APED and issuing CAs, who become aware of Confidential Information, ensure that they are not exposed to risk and that they are not disclosed to third parties.

9.4 Privacy of Personal Information

The Public Key Infrastructure as provided for in this regulation, is subject to the legislation on personal data protection. APED applies a privacy policy which can be found at the following address: https://www.aped.gov.gr

9.4.1 Privacy Plan

APED and issuing CAs implement a policy for the protection of personal data in accordance with the provisions for the protection of personal data, privacy of communications and any other relevant provision. APED and issuing CAs do not disclose nor exploit the names of Subscribers or other personal information, in accordance with §9.3.3.

9.4.2 Information Treated as Private

The legislation for the protection of personal data applies in this case.

9.4.3 Information Not Deemed Private

Subject to applicable laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

The Participants in the PKI of APED and issuing CAs, who are aware of Personal Data, ensure that they are not exposed to risk and not disclosed to third parties and comply with the applicable legislation on personal data protection.

9.4.5 Notice and Consent to Use Private Information

The provisions of the current legislation on the protection of personal data shall apply.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

APED and issuing CAs disclose Confidential Information and Personal Data only in compliance with the relevant legislative framework. The private keys of the Subscriber Signing Certificates that follow the CP are never disclosed to a third party, including APED.

9.4.7 Disclosure upon Owner's Request

APED privacy policy contains provisions relating to the disclosure of private Information to the person disclosing it to APED. This section is subject to applicable privacy laws.

9.5 Intellectual Property Rights

9.5.1 Property Rights in Certificates and Revocation Information

APED and issuing CAs respectively retain all intellectual property rights for the Certificates and revocation information they issue.
APED and issuing Cas respectively grant a non-exclusive, free of charge license to reproduce and distribute the Certificates they issue as long as they are reproduced in full and as long as their use is subject to the General Terms and Conditions. APED and issuing CAs respectively provide revocation information to each Relying Party in accordance with the applicable General Terms and Conditions.

9.5.2 Property Rights in Keys and Key Material

In all cases, the Subscribers' public keys are the intellectual property of the issuing CAs that issue the Certificates

9.5.3 Procedures for the Protection of Subscribers or Relying Parties

APED ensures the Subscriber or Relying Party against failures of the Public Key Infrastructure under the provisions hereof.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

APED and SubCAs guarantee to Subscribers and Relying Parties, as a minimum, that:

- There is no mention of false information in the Certificate that is known or is due to the fault of the entities that approve the Certificate Application or issue the Certificate.
- There are no errors in the elements of the Certificate which were caused by the CAs that approved the Certificate Application or the CAs that issued the Certificate as a result of failure to exercise the utmost care in handling the Certificate Application or creating the Certificate.
- Their Certificates meet all the essential requirements of this CP and the applicable Practice Statement, as well as revocation services and the use of the information space.

9.6.2 RA Representations and Warranties

The RAs of the subCAs guarantee to the Subscribers and the Relying Parties as a minimum that:

- There is no mention of false information in the Certificate which is known or due to their fault.
- There are no errors in the details of the Certificate which were caused by the officers who approved the Certificate Application as a result of a failure to exercise reasonable care in handling the Certificate Application.
- Their Certificates meet all the essential requirements of this CP and the applicable Practice Statement, as well as revocation services and use of the information space.

9.6.3 Subscriber Representations and Warranties

The Subscriber accepts/guarantees, as a minimum, that:

- Each authorized electronic signature created using the private key corresponding to the public key listed on the Certificate constitutes the authorized electronic signature of the Subscriber, provided the Certificate has been accepted and is valid (not expired or revoked) at the time of generation of this authorized electronic signature.
- The private key is protected and no unauthorized person has ever had access to it
- All the assumptions and particulars of the Subscriber in the Certificate Application submitted by the Subscriber are true.
- All information provided by the Subscriber is true.
- The Certificate is used exclusively for approved and lawful purposes, in accordance with all the requirements of this CP and the applicable Practice Statement.
- The Subscriber is not a CA, and therefore does not use its private key corresponding to the public key listed on the Certificate to digitally sign any Certificate (or any other form of certified public key) or CRL, as CA or any other role

9.6.4 Relying Party Representations and Warranties

The Terms of Relying Parties require the latter to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, General Terms and Conditions for Use of Qualified Certificates of issuing Cas, disclaim possible warranties, including any warranty of merchantability or fitness for a particular purpose, subject to the provisions of paragraph 9.2 hereof

9.8 Limitations of Liability

Practice Statements, General Terms and Conditions of Use of Certificates of issuing CAs may, after approval by APED, limit their liability including the exclusion of indirect, extraordinary, incidental and consequential damages.

9.9 Duration and Termination

9.9.1 Start of Validity

The validity of present CP of APED begins with its publication in the Government Gazette. Then, this CP is immediately posted on the network storage area of APED.

9.9.2 End of Validity

Present CP will remain in force until it is replaced by any new, modified version, in accordance with the provisions of paragraph §9.11 hereof.

9.9.3 Effect of Termination

Upon termination of this CP, SubCAs, Participants and Relying Parties of the APED Public Key Infrastructure, continue to be bound by its terms, regarding all certificates issued during the validity of this CP, and for the remainder of their period of validity.

9.10 Individual Notices and Communications with Participants

APED and SubCAs shall use reasonable methods to communicate with each other as well as to communicate with their Subscribers and Relying Parties, when this is needed, taking into account the criticality and subject matter of the communication- information.

9.11 Amendments

Amendments to this CP are allowed after a proposal by APED. The amendments will either be in the form of a document containing the amendments to the CP or a new version of the CP. APED informs Hellenic Telecommunications and Post Commission (EETT) of new or updated versions, in accordance with article 24, par. 2(a) of the EIDAS regulation, publishes them in the Official Gazette and in the Storage Area section of APED for Updates and Announcements on the Regulations at the address: www.aped.gov.gr . New versions of the CP supersede any previous versions.

9.11.1 Information Subject to Change Without Notice

APED may propose amendments hereto without notice to Subscribers and Relying Parties, for changes that are not of material importance, including but not limited to typographical error corrections, URL changes, and contact information changes.

9.11.2 Information Subject To Change With Notice

APED may make substantial amendments to the CP, after informing Hellenic Telecommunications and Post Commission (EETT) and after warning the Subscribers at least with a relevant announcement in its Storage Space reserved for Updates and Announcements on the Regulations at the address: www.aped.gov.gr.

9.11.3 Notice of Amendments

APED announces the amendments to the CP, after informing Hellenic Telecommunications and Post Commission (EETT), in the section of its Storage Space reserved for Updates and Announcements on the Regulations, at the address: www.aped.gov.gr.

9.12 Posting and Communication Policy

9.12.1 Data not published in the CP

Security documents considered confidential by APED and/or issuing CAs are not disclosed to third parties.

9.12.2 Publication of the CP

This CP is published in the Official Gazette and posted in electronic form in the APED Repository at http://pki.aped.gov.gr where it is available in Adobe Acrobat® document format.

9.13 Dispute Resolution

Disputes between APED, issuing CAs, Subscribers and Relying Parties will be resolved in accordance with applicable law by the Greek Courts.

9.14 Applicable Law

The interpretation, validity and application of this CP is governed by the current EU and Greek legislation.

9.15 Force Majeure

APED as well as SubCAs are not responsible for cases of disaster due to reasons of force majeure

B. Certification Practice Statement of Subordinate Certification Authorities of the Hellenic Public Administration Certification Authority

1. Introduction

This Certification Practice Statement (CPS) of the Subordinate Certification Authorities (SubCAs) of the Hellenic Public Certification Authority (APED), specifies the Certificate Policy (CP) of APED for the Certificate Policy (§1.2.1), and in particular the terms and conditions as well as the technical specifications for the approval, issuance, handling, use, revocation and re-keying of the qualified electronic signature certificates of subscribers.

While the CP sets out the requirements that must be met by the participants in the PKI of APED, this CPS describes how APED meets those requirements in accordance with EU Regulation 910/2014 (eIDAS). More specifically, this CPS describes the practices that APED applies for the following:

- the safe management of the PKI and
- the issuing, maintaining and managing of the lifecycle of Qualified Certificates as defined in Regulation (EU) no. 910/2014.

This CPS conforms to Internet Task Force (IETF) RFC 3647 regarding the interpretation of the Certificate Policy and the Certification Practice Statement. Finally, this Certification Practice Statement applies and implements the APED Certificate Policy, unless otherwise specified by the provisions herein.

The CPS will be reviewed once a year.

1.1 Summary

This CPS defines:

- The obligations of the SubCAs, the Registration Authorities, the Subscribers and the Relying Parties.
- The issues related to the General Terms and Conditions of Use of Certificates.
- The methods used to confirm the identity of Subscribers.
- Operational procedures regarding Subscriber's Certificate lifecycle services: request for issuance, acceptance and revocation of Certificate keys.
- The contents of Certificates, Certificate Revocation Lists (CRLs), and Online Certificate Status Protocol (OCSP) Certificates, when available.
- Security operational procedures for control information logging, record keeping and disaster recovery.
- Physical security, personnel security, key management and logical security regulations.
- The management of the CPS, including its modification methods.

APED applies the following sequence for issuing a qualified electronic signature certificate:

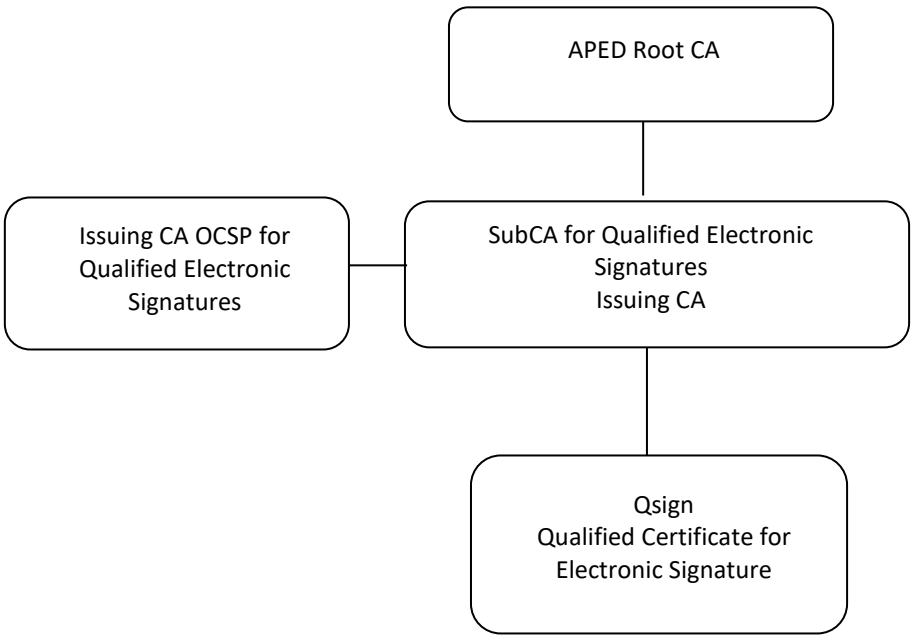


Table 1 includes the list of APED documents to be published, as well as their publication locations. Documents that are not available for publication are confidential material of APED.

Table 1: Regulations Documents Available

Documents	State	Public Post Location
Certification Regulation of the Hellenic Public Administration Certification Authority (APED)	Public	APED Storage Area, in accordance with §2.2 of the CP
Terms and Conditions of Certificate Use	Public	Storage Area of the SubCAs, in accordance with §2.2 of the CP

1.2 Document Name and Identification

The SubCAs have adapted this CPS to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, also known as RFC 3647, of the Action Group for the Internet Engineering Task Force, a body responsible for setting standards on the Internet, to facilitate the depiction of the certificate policy in place. Minor deviations from the structure of RFC 3647 in individual details are necessary due to the application of the CA operational model in the public sector.

1.2.1 Services offered by SubCAs

The SubCAs that implement this CPS manage the life cycle of subscribers' electronic signature certificates (issuance, revocation, suspension and renewal) in accordance with the APED Certification Policy.

1.2.2 Certificate Policy Object Identifier Value

The Certificates issued by the SubCAs in accordance with this CPS include Object Identifier values that correspond to the respective certificate policy being followed. The object specifier value is: 1.2.300.0.110001.1.2.1.1.

1.3 PKI Participants

In accordance with the provisions of §1.3 of the CP of APED.

1.3.1 Certification Authorities

Certification Authority (CA) is the authority trusted by the users of trusted services (i.e., subscribers as well as relying parties) to create and assign certificates. The CA has overall responsibility for the provisions of trusted services.
The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA). PCAs act as roots. APED Certification Authorities that issue Qualified Certificates to Subscribers are Subordinate to the PCA.
APED operates as a Certification Authority that issues Qualified Certificates under the following CA hierarchy:

Primary Certification Authority (PCA) / Root CA
CN = APED Global Root CA
O = APED
C = GR
Serial Number = 6780ecc5cd800b2e85773b1a24324287
Thumbprint = 444dae315d00219c6a152f0cc02aae323bf9c6ac

Qualified Electronic Signature Issuing CA
CN = APED Qualified eSignature Issuing CA
O = HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY
C = GR
Serial Number = 3be7beb6fa604f85b5a9b7b67beb7756
Thumbprint = 4daf5df29ea6dc58c5c41feafcc7a031f9b2f442

APED certificates are issued according to the following certificate policies:

- OID 1.2.300.0.110001.2.1.1 {iso(1) member-body(2) gr(300) elot(0) ypesdda(110001) APED Trust Services (2) APED Qualified Trust Services (1) Qualified Electronic Signature Policy (1)}
- OID 0.4.0.194112.1.0 {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0)}
- OID 0.4.0.194112.1.2 {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd(2)}
- OID 0.4.0.2042.1.1 {tu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp(1)}
- OID 0.4.0.2042.1.2 {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)}

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and validation of Subscribers for issuing Certificates and initiates or accepts revocation requests for Certificates on behalf of the CA. APED acts as an RA for the Qualified Certificates it issues.

APED has the authority to delegate to a third party the responsibility of identifying and validating the Subscriber. In this case, the third party is the Local Registration Authority (LRA-Designated Office). LRA performs its responsibilities in full compliance with this CPS

APED trains the authorized personnel regarding the validation process and the security procedures before starting the relevant activities of the LRAs. APED may carry out audits on the activities and procedures of the LRAs in order to ensure compliance with this CPS.

1.3.3 Local Registration Authorities (LRAs)

A Local Registration Authority (LRA) is an entity that performs the identification and verification of the identity of Subscribers, as well as the initial review of their relevant documents for the issuance and revocation of Certificates. The relationship between the LRA and the CA includes, among others, the following:

- the full details of the authorized LRA employees who will carry out the tasks and activities of the LRA,
- the obligation of the LRA to have its authorized employees receive training from APED regarding the tasks and activities of the LRA, as well as to accept inspections by APED,
- the obligation of the authorized employees of the RLA to use certificates issued by the APED CA in order to ensure secure communication between the parties,
- the obligation of the LRA to process the Subscribers' applications exclusively through the authorized employees of the LRA.

The LRA submits all applications or requests of the Subscriber, accompanied by relevant documents, to the Registration Authority for approval or rejection regarding the issuance or revocation of Certificates.

1.3.3 Subscribers

Subscribers are natural persons, holders of Certificates in accordance with the provisions herein. For the certificates specifically issued according to the CP, the Subscribers must have legal capacity.

1.3.4 Relying Parties

Relying Parties are natural or legal persons who act based on trust in a Certificate issued by APED. The Relying Party may be, or may not be, a Subscriber within the PKI of APED.

1.4 Certificate Usage

In accordance with the provisions of §1.4 of the CP of APED.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS is issued by the Hellenic Public Administration Certification Authority (APED). Any requests for clarification on the chapters herein shall be addressed to the Hellenic Public Administration Certification Authority

1.5.2 Contact Information

Contact information for the SubCAs is published at the following web page:

- www.aped.gov.gr

1.6 Definitions and Acronyms

Appendix A includes Table of Definitions and Acronyms

2. Publication and Repository

2.1 Repositories

In accordance with the provisions of §2.1 of the CP of APED.

2.2 Publication of Certificate Information

APED maintains a web-based repository on a public data communication network (https://pki.aped.gov.gr/repository) that allows Relying Parties to submit online queries regarding revocation and other information regarding the status of Certificate. The CA provides Relying Parties with information on how to search for the appropriate network repository to check the status of the Certificate, as well as how to search for the OCSP responder.

APED publishes in its public information repository the following information at least:

- Overview of the certification hierarchy

- Certification Policies and Certification Practice Statement
- Audit results
- Certificates, including root and issuing CAs
- Profiles
- General Terms and Conditions for use of Qualified Trust Services
- Certificate Revocation Lists
- Certificate search
- Privacy Policies

2.2.1 Publication of CPS

This CPS is published in electronic form at the Repository at https://pki.aped.gov.gr/repository, where it is available in Adobe Acrobat® document format.

2.2.2 Items not published in the CPS

Security documents considered confidential by SubCAs are not disclosed to third parties.

2.3 Time or Frequency of Publication

The SubCAs announce the modifications of the CPS, within a reasonable period of time in their Storage Space, at the addresses mentioned in section §2.2.1.
Subscriber Certificates are published upon issue. Information regarding the status of Certificates is published in accordance with §4.9.6 and §4.9.8 of the CPS.

2.4 Access Controls on Repositories

In accordance with the provisions of §2.4 of the CP of APED.

3. Identification and Authentication

3.1 Naming

Certificates are named as provided in ITU-T Recommendation X.509 [6] or Internet Study Group RFC 5280 [7] and the relevant part of the ETSI EN 319 412 standard.

3.1.1 Type of Names

The type of names assigned to the CA and Subscribers is described in the relevant Certificate Profile documentation publication in the APED repository. The APED CA and Subscriber Certificates include the X.501 Distinguished Names in the Issuer and Subject fields.

3.1.2 Need for Names to be Meaningful

In accordance with the provisions of §3.1.2 of the CP of APED.

3.1.3 Anonymity or Pseudonymity of Subscribers

SubCAs do not issue certificates where a pseudonym is written in the Subscriber's details

3.1.4 Uniqueness of Names

In accordance with the provisions of §3.1.4 of the CP of APED.

3.2 Initial Registration

3.2.1 Method to Prove Possession of Private Key

In accordance with the provisions of §3.2.1 of the CP of APED

3.2.2 Authentication of Identity of Natural Person

In accordance with the provisions of §3.2.2 of the CP of APED

3.2.3 Non-Verified Subscriber information

In accordance with the provisions of §3.2.3 of the CP of APED

3.3 Identification and Authentication for Re-keying Requests

3.3.1 Identification and Authentication for Routine Re-Keying

Not applicable

3.3.2 Identification and Authentication for Re-Keying after revocation

In accordance with the provisions of §3.3.2 of the CP of APED

3.4 Identification and Authentication for Revocation Request

To revoke Subscriber Certificates, it is necessary to identify the Subscriber according to the procedures described in §4.9.3. Specifically, to verify the identity of a Subscriber's revocation request, one of the following acceptable procedures is followed on a case-by-case basis:

- Login and authentication of the Subscriber at the online address https://services.aped.gov.gr/apedcitizen/login/ , and input of the personal eight-digit certificate issuance/ revocation code in the corresponding field of the revocation request.
    - If the Subscriber has not saved or does not remember the personal issuance / revocation code, a reminder can be sent. In this case, he enters his Tax Identification Number and date of birth and if these details are verified, an SMS with the code is sent to the mobile phone registered when the certificate was issued. If he has changed his mobile phone number, the registered mobile phone cannot be modified and he cannot receive the reminder code.
- Registration of an Application-Declaration of revocation at gov.gr. The Subscriber then logs in and is authenticated at the online address https://services.aped.gov.gr/apedcitizen/login/ and submits a revocation request using the verification identification number (code) of the Application-Declaration at gov.gr. The request is routed to the Registration Authority for approval.
- Revocation in the event of failure of the application:
  https://services.aped.gov.gr/apedcitizen/login/
  In case of failure of the above application, due to a sudden and unforeseen event, the Subscriber may submit a revocation request by issuing an application/ Declaration form of revocation of a qualified certificate from the Single Digital Portal of the Public Administration (gov.gr) and sending it via e-mail to the e-mail address aped@mindigital.gr or by traditional mail to the Ministry of Digital Governance/APED, 11 Frangoudi str and Al. Pantou, Postal Code 17671.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL

4.1 Certificate Issuance Application

4.1.1 Who Can Submit a Certificate Issuance Application

In accordance with the provisions of §4.1.1 of the CP of APED

4.1.2 Enrollment Process and Responsibilities

For the issuance of Subscriber Certificates, all Subscribers are subject to a registration and identity verification process, which consists of:

- Authentication and login to the electronic qualified certificate management application (https://services.aped.gov.gr/apedcitizen/login/), and submission of an electronic request for the issuance of a certificate by filling in all the mandatory fields.
- Either remote identification or physical presence of the Subscriber himself at the competent LRA Office or, if deemed necessary, at representatives of the Registration Authority or the Certification Authority, to confirm the Subscriber's identity.
- Submission of a certificate request.
- Written or electronic acceptance of the Certificate Terms and Conditions of Use.
- Creation or submission of a request to create a key pair according to §6.1 of the CP.
- Sending of the public key by the Subscriber, to the issuing CA, according to §6.1.3 of the CP.
- The Subscriber's proof to the issuing CA, in accordance with §3.2.1 of the CP, that he is in possession of the private signing key corresponding to the public key he sent to the issuing CA.

4.2 Certificate Issuance Application Processing

4.2.1 Approval or Rejection of Application of Subscriber’s Certificate Issuance

Approval or rejection of the request for the Subscriber’s Certificate Issuance is conducted in accordance with the provisions of §4.2.1 of the CP of APED

4.2.2 Χρόνος Επεξεργασίας Αιτήσεων

In accordance with the provisions of §4.2.3 of the CP of APED

4.3 Certificate Issuance

After the approval of the request for the issuance of a qualified electronic signature certificate, the Subscriber receives a message (SMS) from the RA through an automated process about the positive result of the processing of the application he submitted. The message is sent to the mobile phone number entered in the certificate application submitted.

The Subscriber must then connect to the electronic application for managing qualified certificates and proceed to create and issue the qualified electronic signature certificate in the QSCD in his possession.

4.3.1 Issuing CA Actions during Certificate Issuance

In accordance with the provisions of §4.3.1 of the CP of APED

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Issuing CAs inform Subscribers about the process of issuing qualified electronic signature certificates, about their availability and how to receive them from the address http://www.aped.gov.gr . The relevant information is also available to the interested party after logging into the qualified certificate management application (https://services.aped.gov.gr/apedcitizen/login/).

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

In accordance with the provisions of §4.4.1 of the CP of APED.

4.4.2 Publication of the Certificate by the CA

In accordance with the provisions of §4.4.2 of the CP of APED.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

In accordance with the provisions of §4.5.1 of the CP of APED.

4.5.2 Relying Party Public Key and Certificate Usage

In accordance with the provisions of §4.5.2 of the CP of APED.

4.6 Certificate Renewal

Not applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

In accordance with the provisions of §4.7.1 of the CP of APED.

4.7.2 Who May Request Certification of a New Public Key

In accordance with the provisions of §4.7.2 of the CP of APED.

4.7.3 Processing Certificate Re-Keying Requests

In accordance with the provisions of §4.7.3 of the CP of APED.

4.7.4 Notification of New Certificate Issuance to Subscriber

The notification of the issuance of a Certificate with regenerated keys to the Subscriber is carried out in accordance with the provisions of §4.3.2 of the CPS.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

In accordance with the provisions of §4.7.5 of the CP of APED.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Issuing CAs publish re-keyed certificates in an information space accessible to the public, in accordance with §4.4.2 of the CPS

4.8 Certificate Modification

In accordance with the provisions of §4.8 of the CP of APED.

4.9 Certificate Revocation

4.9.1 Circumstances for Revocation

In accordance with the provisions of §4.9.1 of the CP of APED.

4.9.2 Who Can Request Revocation

In accordance with the provisions of §4.9.2 of the CP of APED.

4.9.3 Procedure for Revocation Request

The revocation service is available 7 days a week, 24 hours a day. A Subscriber who wishes to revoke his Certificate must submit a revocation request in the following ways:

- At the address https://services.aped.gov.gr/apedcitizen/login/, where the submission of the request is only allowed after authentication in the system and by using the personal qualified certificate issuance / revocation code in the corresponding field of the revocation request.
- With a Declaration Statement of revocation at gov.gr and an application at https://services.aped.gov.gr/apedcitizen/login/ . The application is then forwarded to the Registration Authority for approval.
- Revocation in the event of failure of the application:
  https://services.aped.gov.gr/apedcitizen/login/
  In case of failure of the above application, due to a sudden and unforeseen event, the Subscriber may submit a revocation request by issuing an application/ Declaration form of revocation of a qualified certificate from the Single Digital Portal of the Public Administration (gov.gr) and sending it via e-mail to the e-mail address aped@mindigital.gr or by traditional mail to the Ministry of Digital Governance/APED, 11 Frangoudi str and Al. Pantou, Postal Code 17671.

4.9.4 Time within Which CA Must Process the Revocation Request

In accordance with the provisions of §4.9.4 of the CP of APED.

4.9.5 Revocation Checking Requirements for Relying Parties

In accordance with the provisions of §4.9.5 of the CP of APED.
In particular, the CRLs of the issuing CAs are available from the address https://pki.aped.gov.gr/repository.

4.9.6 CRL Issuance Frequency

In accordance with the provisions of §4.9.6 of the CP of APED.

4.9.7 Maximum Latency for CRLs

In accordance with the provisions of §4.9.7 of the CP of APED.

4.9.8 On-Line Revocation/Status Checking Availability

Information on the status of Certificates issued by issuing CAs is also available through the use of the Online Certificate Status Protocol (OCSP).

4.9.9 On-Line Revocation Checking Requirements

In accordance with the provisions of §4.9.9 of the CP of APED.

4.9.10 Other Forms of Revocation Advertisements Available

In accordance with the provisions of §4.9.1 of the CP of APED.

4.9.11 Special Requirements regarding Key Compromise

In accordance with the provisions of §4.9.11 of the CP of APED.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of the Certificates is available through the addresses defined in §4.9.5 for the CRL and §4.9.8 for the OCSP Responder.

4.10.2 Service Availability

In accordance with the provisions of §4.10.2 of the CP of APED.

4.11 End of Subscription

In accordance with the provisions of §4.11 of the CP of APED.

5. Physical, Management and Operational Protection and Security Measures

In accordance with the provisions of §5 of the CP of APED.

6. Technical Security Controls

In accordance with the provisions of §6 of the CP of APED.

7. Certificate, CRL and OCSP Profiles

In accordance with the provisions of §7 of the CP of APED.

8. Compliance Audit and Other Assessments

In accordance with the provisions of §8 of the CP of APED.

9. Other Business and Legal Matters

9.1 Fees

In accordance with the provisions of §9.1 of the CP of APED.

9.2 Financial Responsibility

In accordance with the provisions of §9.2 of the CP of APED.

9.3 Confidentiality of Information

In accordance with the provisions of §9.3 of the CP of APED.

9.4 Privacy of Personal Information

In accordance with the provisions of §9.4 of the CP of APED.

9.5 Intellectual Property Rights

In accordance with the provisions of §9.5 of the CP of APED.

9.6 Representations and Warranties

In accordance with the provisions of §9.6 of the CP of APED.

9.7 Disclaimers of Warranties

In accordance with the provisions of §9.7 of the CP of APED.

9.8 Limitations of Liability

In accordance with the provisions of §9.8 of the CP of APED.

9.9 Duration and Termination

9.9.1 Start of Validity

The validity of present CPS begins with its publication in the Government Gazette. Then, this CPS is immediately posted on the network storage area of the SubCA.

9.9.2 End of Validity

Present CPS will remain in force until it is replaced by any new, modified version, in accordance with the provisions of paragraph §9.11 hereof.

9.9.3 Effect of Termination

Upon termination of this CPS, SubCA, Participants and Relying Parties of the APED Public Key Infrastructure, continue to be bound by its terms, regarding all certificates issued during the validity of this CPS, and for the remainder of their period of validity.

9.10 Individual Notices and Communications with Participants

In accordance with the provisions of §9.10 of the CP of APED.

9.11 Amendments

In accordance with the provisions of §9.11 of the CP of APED.

9.12 Posting and Communication Policy

In accordance with the provisions of §9.12 of the CP of APED.

9.13 Dispute Resolution

In accordance with the provisions of §9.13 of the CP of APED.

9.14 Applicable Law

The interpretation, validity and application of this CPS is governed by the current EU and Greek legislation.

9.15 Force Majeure

In accordance with the provisions of §9.15 of the CP of APED.

C. Certificate Policy & Certification Practice Statement for Time Stamping Services

1. Introduction

With the present APED Certification Regulation, the terms, conditions and procedures for the provision of trust services by the Hellenic Public Administration Certification Authority (APED) are determined, in accordance with article 58 of Law 4727/2020. APED provides time stamping services in order to create the necessary evidence for the existence of a set of digital data at a specific time. APED's Time Stamping Certificate Policy and Certification Practice Statement have been merged into this section, the provisions of which define the policies and practices applied to the provision of time stamping services by APED, as a Time Stamping Service Provider.

APED implements a trusted and reliable system of accurate time for the provision of time stamping services and takes all necessary measures to ensure the confidentiality and maintain the integrity of the private cryptographic keys as Time Stamping Service Provider.
This section, on one hand, specifies the Certificate Policy of APED regarding the Qualified Time Stamping Services provided by it, on the other hand, it defines the Certification Practice Statement of the Time Stamp Authority.

2. General Concepts

2.1 Time Stamping Services

Qualified Time Stamping Services (QTSS) of APED consist of infrastructure management and Time Stamp provisioning. They are provided by the APED Time Stamping Authority (TSA) to the Relying Parties and are an integral part of the APED Public Key Infrastructure (PKI) and are compliant with EU Regulation 910/2014 (eIDAS) and the European Telecommunications Standards Institute (ETSI). Authorized Time Stamping Services ensure the use of a reliable time source and proper management of all system components.

2.2 Time Stamping Authority

APED Time Stamping Authority is responsible for providing a Qualified Time Stamping Service as described in this document. It is responsible for the operation of the relevant Time Stamping Units (TSU) that are created and signed on behalf of the TSA. The legal entity responsible for the TSA is APED acting as Qualified Timestamping Services Provider (QTSP)
APED issues Qualified Time Stamps under the following hierarchy:

Root CA
CN = APED Global Root CA
O = APED
C = GR
Serial Number = 6780ecc5cd800b2e85773b1a24324287
Thumbprint = 444dae315d00219c6a152f0cc02aae323bf9c6ac

Time Stamping Authority CA
CN = APED Qualified Time Stamping Issuing CA
O = HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY
C = GR
Serial Number = 28901421ae97b7d47c4cc4eb60ea0597
Thumbprint = 59cd4e7b30478a8c907459f0a38337d1d64ce4e3

APED TSA and TSU certificates are issued according to the following certificate policies:

- OID 1.2.300.0.110001.2.1.2: {iso(1) member-body(2) gr(300) elot(0) ypesdda(110001) APED Trust Services (2) APED Qualified Trust Services (1) Qualified Time Stamping Policy (2)}
- OID 0.4.0.2023.1.1: {itu-t(0) identifiedorganization(4) etsi(0) time-stamp-policy(2023) policyidentifiers(1) baseline-ts-policy (1)}
- OID 0.4.0.2042.1.2: {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)}

Certificate QcStatements:

- OID 0.4.0.1862.1.1: {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1)}
- OID 0.4.0.1862.1.4: {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) 4}
- OID 0.4.0.1862.1.5: {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcPDS(5)}

2.3 Subscribers

Subscribers are natural persons, holders of qualified electronic signature certificates, to whom the time stamp is provided

2.3.1 Relying Parties

A Relying Party is an individual or entity that receives a time-stamped digital document and acts in reliance of a certificate and/or digital signature issued under the TSA. A Relying Party must evaluate the correctness and validity of the document itself in the context in which it is used.

2.3.2 Other Participants

Not applicable.

2.3.3 Time Stamps Usage

The Time Stamps issued by APED, as specified in this document, are qualified in accordance with paragraph 34 of article 3 of the eIDAS Regulation. Time Stamps shall be used only to the extent that their use is in accordance with applicable law and within the limits and context set forth herein. Any use outside of these limits or for illegal purposes or contrary to the public interest or for purposes that may harm APED is prohibited. For example, the use of Time Stamps is prohibited for any of the following purposes:

- unlawful activity (including cyber-attacks);
- issuance of new Time Stamps and information regarding Time Stamp validity;
- using the Time Stamp issued to time-stamp documents which can bring about unwanted consequences (including time-stamping such documents for testing purposes).

2.4 Time Stamping Policy and TSA Practice Statement

2.4.1 Purpose

This section specifies the policy and security requirements related to the operational and management practices of APED as a Time Stamp Authority (TSA) for the issuance of Qualified Time Stamps. These can be used to support electronic signatures or in any application that requires proof that a datum existed before a certain point in time. In addition, it can be used by independent entities as a basis to confirm that APED TSA is a trusted entity for issuing Qualified Time Stamps in accordance to the eIDAS Regulation.

2.4.2 Level of Specificity

The present document describes only general rules of issuing and managing Time Stamp Tokens (TST). Detailed description of the infrastructure and related operational procedures are included in additional documents that are not made publicly available

3. Time Stamp Policies

3.1 Overview

The Time Stamp Policy is a set of rules regarding the issuance and management of the Time Stamps produced by APED as the QTSSP for Subscribers. Time Stamping services include organizing the infrastructure and issuing Time Stamp Tokens (TST). The specific services are provided by APED to Subscribers as part of the operation of APED's public key infrastructure. The services are mainly provided to support Qualified Electronic Signatures but also for any application that requires evidence for the existence of some data at a specific time. APED ensures the use of a reliable time source and the appropriate management of Time Stamping systems.
Time Stamps are issued by APED through the following link: https://timestamp.aped.gov.gr/qtss.
This Policy defines the set of rules used when issuing a TST and regulates the security level of the TSA of APED. TSA APED issues TSTs according to the ETSI EN 319 422 standard. TSTs are issued with an accuracy of one (1) second. Time Stamps are requested via Hypertext Transfer Protocol (HTTP), as described in RFC 3161.

3.2 Identification

The object-identifier (OID) of the Certificate Policy & Certification Practice Statement for Qualified Time Stamping Services of APED is 1.2.300.0.110001.2.1.2.
This OID is referenced in every APED issued time-stamp token, and the Certificate Policy & Certification Practice Statement for Qualified Time Stamping Services of APED is available to both Subscribers and Relying Parties.
Certificate Policy & Certification Practice Statement for Qualified Time Stamping Services of APED are based on ETSI best practice for time-stamping policy (OID 0.4.0.2023.1.1).

3.3 User Community and Applicability

There are no limitations on the eligibility of users or the applicability of the services delivered. APED TSA may provide Electronic Data Time Stamp Services to any user, including closed communities.

3.4 Conformance

APED TSA uses the identifier in TST as given in section 3.2 “Identification”.
APED TSA ensures compliance of provided services with regulations specified in section 4.1 “TSA Obligations to Subscribers” and ensures reliability of control mechanisms described in the Practice Statement section herein.

4. Obligations and Liability

APED guarantees and ensures the implementation of the Time Stamp Policy in accordance with the provisions of section 3, as well as the requirements of the "Certification Practice Statement of TSA" section.
In particular, regarding Subscribers and Relying Parties, APED ensures that the maximum deviation from the UTC clock of the source is one (1) second.
Subscribers and relying parties are responsible for verifying the validity and correctness of the time stamp.

4.1 TSA Obligations towards Subscribers

APED guarantees the availability of 99.00% of APED TSA services, operation 24 hours a day / 7 hours a week, excluding planned technical outages related to equipment and system maintenance.
APED undertakes the following obligations to TSA Subscribers:

- To operate in accordance with this APED Time Stamping Services Certificate Policy & Certification Practice Statement and other relevant operational policies and procedures.
- To ensure that TSUs maintain a minimum UTC time accuracy of ± 1 second.
- To ensure on a permanent basis the physical and logical security, as well as the integrity of materials, software and databases required for the correct functioning of the TSS.

- To monitor and control the TSS and the whole TSA infrastructure, in order to prevent or limit any disturbance or unavailability of the TSS.
- To undergo internal and external reviews to assure compliance with relevant legislation.
- To provide high availability access to APED TSA systems except in the case of planned technical interruptions and loss of time synchronization.

4.2 Subscriber Obligations

Subscribers should verify the signatures created by APED TSA on the TST.
Such verification includes:

- Verification whether the TSA signature on the TST is valid.
- Verification of the TSA certificate:
    - Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself)

4.3 Relying Party Obligations

Relying parties should verify the signatures created by APED TSA on the TST
Such verification includes:

- Verification whether the TSA signature on the TST is valid.
- Verification of the TSA certificate:
    - Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself)
    - Verification whether the certificate is not expired at the moment of TSA signature
    - Verification whether the certificate was not revoked at the moment of TSA signature

Relying Parties should take into account any limitations on usage of the time stamp indicated by the APED Time Stamping Services Certificate Policy & Certification Practice Statement. If the verification takes place after the end of the validity period of the Certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421.

4.4 Liability

The Greek State is liable for damage caused by acts or omissions of the APED bodies or the issuing CAs to any natural or legal person, due to non-compliance with the obligations provided for in this regulation, in accordance with article 105 of the Introductory Law of the Civil Code.
General Terms and Conditions for the use of Qualified Trust Services limit the liability of APED. Limitations of liability include the exclusion of indirect, special, incidental and consequential damages. Limitations of liability are the same regardless of the number of Time Stamps or claims associated with them. In particular, for the responsibility of the Greek State due to actions or omissions of the bodies of APED, in terms of compliance with the provisions of the present, the following apply:
The Greek State is not responsible for any malfunction of APED services in cases of force majeure, such as, indicatively, 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 "Liability and burden of proof" of Regulation 910/2014 apply in this case, pursuant to paragraph 3 of the same article.

5. Certification Practice Statement of TSA

5.1 Practice and Disclosure Statements

APED Certification Practice Statement describes how Time Stamping Policy is implemented, the process for establishing the Time Stamping Service and maintaining the accuracy of the clock.
ADEP ensures that:

- all TSA control and event logs, related to the Time Stamping Unit certificate, are kept for at least seven (7) years after the expiry of the TSU certificate.
- all TSA audit and event logs related to the time stamp service are retained for at least one (1) year after the expiration of the TSU Certificate.

TSU certificates are valid for five (5) years. They are replaced every one (1) year.

Time Stamping Server cryptographic keys and certificates are generated, stored, and used in a secure Hardware Security Module (HSM) to perform key signing functions that is at least compliant with FIPS140-2 level 3 or equivalent EAL4+ or higher according to ISO/IEC15408 specifications.
The Certificates of the Time Stamping Servers are published in the relevant directory of the APED PKI (https://pki.aped.gov.gr/repository)
The profile of the key fields of the APED time stamping certificate is described in Table 1.

Table 1. Profile of key fields of Time Stamping Certificate.

Field	Value or Value Constraint
Version	3
Serial Number	Unique value for each Issuer DN
Signature Algorithm	SHA256withRSAEncryption
Issuer DN	cn=APED Qualified Timestamping Issuing CA ou=APED PKI Services o=HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY c=GR
Validity Start	Based on Universal Coordinate Time
Validity End	Based on Universal Coordinate Time. The validity period does not exceed the validity period of the certificate of the Primary Certification Authority.
Subject DN	cn=APED Qualified Timestamping Unit ou=APED PKI Services o=HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY c=GR
Key Size	2048 bits
Key Usage	Digital Signature, Non-repudiation
Extended Key Usage	Time Stamping

APED TSA communicates to all Subscribers and potential Relying Parties the terms and conditions regarding the use of Time Stamping Services of APED. TSA Disclosure Statement of APED complies with the requirements of ETSI EN 319 421.
Some elements of the APED TSA Disclosure Statement are listed below:

- Each TST issued by TSA of APED includes the policy identifier defined in section 2.2 of this document.
- The hashing functions used in the Time Stamping process are compliant with the SHA-256 and SHA-512 regulatory requirements.
- The expected period of validity of APED TSU is up to five (5) years.
- The accuracy of the time provided in a TST is regulated in section 3.1 of this document.
- Application restrictions related to the TSA system are defined in section 3.3 of this document.
- The verification of the TST must be done using the appropriate software.
- The obligations of Subscribers are described in section 4.2 of this document.
- The obligations of the Relying Parties are described in section 4.3 of this document.

- APED keeps secure records related to the operation of the TSA of APED.

5.2 Key Management Life Cycle

APED, as the Primary Certification Authority (PCA), signs the Certificate of the Time Stamping Authority of Qualified Electronic Time Stamps. The APED and Time Stamping Authority Certificates are available to Subscribers and Relying Parties online through the APED repositories, and also as part of the certificate chain which is embedded in the time stamp certificate.

5.2.1 TSA Key Generation

The generation of the TSU signing keys is performed by authorized personnel in a physically secure environment in accordance with CA practices. The creation of the signature keys of the TSU is carried out in secure cryptographic devices, which meet the conditions defined in §5.1 of the CP/CPS of the TSA. Key pairs are generated using secure algorithms and parameters, in accordance with the recommendations of ETSI TS 319 312. The activities performed in each key generation are recorded, dated and signed by all parties involved. These records are retained for inspection and monitoring purposes for a period deemed appropriate by APED.

5.2.2 TSU Private Key Protection

APED takes necessary measures to ensure that the private keys of the TSU remain confidential and maintain their integrity. The TSU's private keys are stored in a secure Hardware Security Module (HSM) to perform key signing functions, which meets the conditions set out in §5.1 of the CA's CP/CPS. There are special checks to ensure that the hardware has not been corrupted and is working properly. TSU private keys cannot be exported in any form and are not accessible outside the Hardware Security Module.

APED creates backup copies of the TSU private keys, for routine recovery and disaster recovery purposes. Such keys are stored in an encrypted form inside cryptographic hardware modules, which ensure an equivalent level of security to the original one. The cryptographic units used to store private keys meet the requirements of this CPS. Private keys are copied to backup hardware cryptographic modules. Restoring TSU key backups requires dual control in a physically secure environment.

5.2.3 TSU Public Key Distribution

APED TSU Public Keys are made available in a Qualified Certificate.
APED TSU Certificates are available for secure download via the APED Repository website https://pki.aped.gov.gr/repository. They can also be found in the European Union's Trusted List of Certification Service Providers via the National Supervisory Authority (Hellenic Telecommunications & Post Commission - EETT).

5.2.4 Rekeying TSU's Key

The operation period for TSU key pairs is defined by setting a private key usage period within the TSU's public key certificate.
APED TST are signed with APED TSU certificates of five (5) years validity. APED TSU certificates of five (5) years validity are only used to sign TST during a usage period of one (1) year.
APED TSU rekey procedure is executed upon expiry of the usage period (1 year) of the TSU certificate. Public keys are archived for a period of at least ten (10) years from the expiration date of the certificate.

5.2.5 End of TSU Key Life Cycle

APED TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place before a TSU's key usage period expires, and that TSU private keys or any part, including any copies are destroyed such that the private key cannot be retrieved.
TST generation system shall reject any attempt to issue a TST if the signing private key is expired or if the signing private key usage period is expired.

5.2.6 Life Cycle Management of the Cryptographic Module used to Sign Time Stamps

APED TSA ensures the security of the HSM throughout its lifecycle.
APED has in place procedures to ensure that:

- Hardware Security Modules are not tampered with in shipment or storage.
- Acceptance testing is performed to verify that cryptographic hardware is performing correctly.
- Installation, activation and duplication of TSU's signing keys in HSMs is done only by personnel in trusted roles, in a physically secure environment.
- TSU private signing keys stored on HSM are erased upon device retirement in accordance with the manufacturer's instructions.

5.3 Time Stamping

5.3.1 Time Stamp Token

APED has in place technical procedures to ensure that TST are issued securely and includes the correct time. Each TST includes:

- a representation of the datum being time-stamped as provided by the applicant
- a unique serial number which can be used for the ordering as well as the identification of a specific TST
- a unique identifier of the policy as described in section 2.2 of the present document
- an electronic signature generated using a key used exclusively for Time Stamping
- an identifier for the TSA and the TSU.
- date and time value traceable to the real UTC time value
- signature algorithm used in TST as set forth in section 5.1 hereof

APED TSUs maintain audit logs for all calibrations against the UTC references

5.3.2 Clock Synchronization with UTC

APED TSA ensures that its time is synchronised with UTC within the declared accuracy with multiple independent time sources. APED TSA incorporates the time in the TST with the accuracy described in section 4.1 of the present document.

Audit and calibration records of the synchronization are maintained by APED. APED TSA ensures that if the time that would be indicated in a TST drifts or jumps out of synchronization with UTC, this will be detected. If the TSU time drifts outside the declared accuracy, and recalibration fails, the TSA will not issue time-stamps until correct time is restored.

APED implements security controls preventing unauthorised operation, aimed at calibration of TSA time.

5.3.3 Leap Second handling procedure

A leap second is an adjustment to UTC by skipping or adding an extra second on the last second of a UTC month. First preference is given to the end of December and June, and second preference is given to the end of March and September.

APED monitors that synchronization is maintained when a leap second occurs.

5.4 TSA Management and Operation

5.4.1 Security Management

APED TSA ensures that administrative and management procedures are applied which are adequate and correspond to recognized best practices. APED performs all TSA functions using trustworthy systems.

5.4.2 Personnel Security

APED maintains appropriate personnel controls fulfilling security best practice and the requirements of relevant standards.
APED personnel possess the appropriate skills and knowledge of Time Stamping, qualifiedsignatures and Trust Services as well as security procedures for personnel with security responsibilities, information security and risk assessment.
Regarding Trusted Persons, the provisions mentioned in section 5.2 of the CP (Section A of this document) of the APED apply.

5.4.3 Physical and Environmental Security

APED TSA implements the Physical Security Policy of APED, as defined in section 5.1 of the APED CP (Section A of this document).

5.4.4 Operations Management

APED TSA acts in accordance with the provisions of paragraph 9 of the APED Certification Regulation as applicable, as well as ETSI EN 319 421 for incident management.

5.4.5 Trustworthy Systems Deployment and Maintenance

APED ensures that the systems maintaining TSA software and data files are trustworthy systems, secure from unauthorized access and modification

5.4.6 Compromise of TSA Services

In the case of compromise to a TSU operation (e.g., TSU key compromise), suspected compromise or loss of calibration, the TSU shall not issue time-stamps until steps are taken to recover from the compromise. In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp, APED makes available to all Subscribers and Relying Parties a description of compromise that occurred.
In case of major compromise of the TSA operation, APED shall make available to all Subscribers and Relying Parties information which can be used to identify the time-stamps which may have been affected, unless this breaches the privacy of the TSA users or the security of the TSA services.

5.4.7 TSA Termination

The TSA is terminated:

- with a decision of the authority exercising supervision over the supply of the service;
- with a judicial decision;
- upon the liquidation or termination of the operations of APED.

Η λειτουργία της ΑΧ τερματίζεται με:

- απόφαση της αρχής που ασκεί την εποπτεία της παροχής της υπηρεσίας
- δικαστική απόφαση
- εκκαθάριση ή διακοπή των λειτουργιών της ΑΠΕΔ

APED ensures that potential disruptions to Subscribers and Relying Parties are minimized, as a result of the cessation of APED services and, in particular, it ensures the continued maintenance of information required to verify the correctness of Trust Services.

In the event that it is necessary for APED TSA to cease operation, APED makes a reasonable effort to notify Subscribers and Relying Parties in advance of the TSA termination. APED TSA revokes the TSU's certificates when it terminates its services.

5.4.8 Compliance with Legal Requirements

APED ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,
- Personal Data laws and EU Regulations,
- Related European Standards:
  - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
  - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
  - ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;
  - ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
  - ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-Stamping Protocol and Time-Stamp Token Profiles

APED acting as QTSP accepts compliance audit for its TSA Services to ensure it meets the eIDAS requirements.

5.4.9 Recording of Information Concerning Operation of Time Stamping Services

APED TSA ensures that all relevant information concerning the operations of the APED Time Stamping Services is recorded for a defined period, in particular for providing evidence for the purposes of legal proceedings.
APED maintains records of all relevant information concerning the operation of the APED TSA for the time period of seven (7) years. APED TSA maintains records of:

- Synchronization of clocks used in time-stamping
- Detection of loss of synchronization
- Time-stamp requests and created time-stamps
- Events relating to the lifecycle of TSU keys and Certificates.

5.4.10 Organizational

APED TSA ensures that its organization is reliable, as required in ETSI EN 319 421.
Policy and Practice documents for the APED TSA are available at https://pki.aped.gov.gr/repository

APPENDIX A – References, Acronyms and Definitions

References

The following documents are relevant to the present Certification Regulation of APED:

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[3] ETSI EN 319 421: “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.

[4] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[5] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[6] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[7] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for trust service providers issuing EU qualified certificates".

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 APED 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 qualified 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 (End User)	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

From the entry into force of this document, any previous decision regulating the subject matter of this document in a different way is repealed.

This Ministerial Decision is valid from its publication in the Government Gazette. This Ministerial Decision to be published in the Government Gazette.