General Terms and Conditions for Use of Qualified Trust Services

(Qualified Certificates for Electronic Signatures, Seals & Time Stamps)

Version 4.0

Valid from 17.02.2021

Version History

Date	Version	Changes
24.02.2017	1.0	Initial document
29.06.2018	1.1	Minor changes in section 11
10.01.2019	2.0	Document title change, Changes to include Qualified time stamping services in par. 1.5, 3.2, 4.2, Changes in Section 5 & 8, Addition of version history section.
25.01.2019	3.0	Addition of par. 1.6, 1.8, 5.5, 5.6 to include Remote ID verification, minor changes in par. 1.4, 7.4.2. and 8.4, added par. 8.7 and 5.3.6
08.02.2019	3.1	Changes in par. 2.3, 4.1, 8.7
25.02.2019	3.2	Added par. 1.5, 5.3.11, changes in par.2.3
26.06.2019	3.3	Minor changes in par. 1.4, 2.3, 9.3 and 15.1
01.04.2020	3.4	Changes in par. 1.2, 1.3, 1.5, 1.8, 1.9, 5.3.8, 5.5, 5.6, 8.8, 9.1
20.05.2020	3.5	Changes in par. 1.5, 1.8, renumbering in par. 5.5 and 5.6
17.02.2021	4.0	Changes in definitions and in par. 1.4, 1.5, 1.8, 5.2, 5.4, 8.4, 8.5, 8.7, 8.8, 10.1 13.2, 13.3, 14.2, Addition of par. 1.10-1.14, 5.5 (after renumbering)

Definitions and Acronyms

Term/Acronym	Definition
Certification Authority (CA)	A part of ADACOM structure responsible for issuing and verifying Certificates and Certificate Revocation Lists with its electronic signature.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Policy (CP)	Symantec Certificate Policy for Qualified Certificates
Certification Practice Statement (CPS)	The document that states the practices that ADACOM as a Trusted Service Provider employs in providing certification services for Qualified Certificates for electronic signatures and Qualified Certificates for electronic seals.
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that have been revoked by the certificate issuer.
Coordinated Universal Time (UTC)	Time scale based on the second as defined in ITU-R Recommendation TF.460-5
eIDAS Regulation	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.
EBA	European Banking Authority
Identity verification / validation	Unique identification of a person by checking his/her alleged identity.
Local Registration Authority (LRA)	An entity that performs the identification and validation of Subscribers and Subjects and the initial examination of their respective documents for the issuance, re-keying and revocation of Certificates.
Long-lived Certificate	A Qualified Certificate which is valid for 1 to 3 years.
National Competent Authority (NCA)	Authority who ensures and monitors effective compliance with Directive (EU) 2015/2366 (Payment Services Directive II).
OCSP	Online Certificate Status Protocol.
OID	An identifier used to uniquely name an object.

PIN code	Activation code for the Qualified Certificates for Electronic Signatures and for Electronic Seals.
PSD2	Directive (EU) 2015/2366 (Payment Services Directive II)
PSP	Payment Service Provider
Private Key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures 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.
Qualified Certificate	Qualified Certificate is a Certificate issued by a CA which has been accredited and supervised by authorities designated by a EU member state and meets the requirements of eIDAS.
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Electronic Seal	Advanced electronic seal, that is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.
Qualified Electronic Time Stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter existed at that time, in such a way that the possibility of the data being changed is precluded, it is based on an accurate time source linked to UTC and is signed using an advanced electronic signature or advanced electronic seal of the Qualified Trust Service Provider.
Qualified Signature/Seal Creation Device (QSCD)	A Secure Signature/Seal Creation Device that meets the requirements laid down in chapter II of the eIDAS Regulation. QSCD can be either local in the form of a USB token or a smart card or remote in the form of a Hardware Security Module.
Qualified trust service	A trust service, as defined in eIDAS Regulation, that meets the applicable requirements laid down in this Regulation.
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 that performs identity verification and validation of Subscribers for issuing Certificates, initiates or passes along revocation requests for Certificates, and approves applications for re-keying certificates on behalf of the CA.
Relying Party	Entity that relies on the information contained within a Certificate.
Remote ID verification	The method/process by which the Subscriber is identified through a video conference and is equivalent to identity verification through physical presence.
Short-lived Certificate	A Qualified Certificate which is valid from 24 to 72 hours and can be used for one transaction.
Subject	The natural person named in a Qualified Certificate for electronic signature, who is associated with a legal person.
Subscriber	An entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations. Subscriber can be either a natural or a legal person.
General Terms and Conditions for Use of Qualified Trust	Present document that sets forth the terms and conditions under which a natural or legal person acts as a Subscriber and/or as a Subject or as a Relying Party and ADACOM provides the corresponding Trust Services.

Services	
Time Stamping Authority (TSA)	The Authority of the Time Stamping Services which issues Time Stamp Tokens.
Time Stamp 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.
Time Stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single Time Stamp Token signing key active at a time.
Trusted List	List containing information about qualified trust service providers in the EU, as well as information on the qualified trust services provided by them.

1. General Terms

Present Terms and Conditions describe main policies and practices followed by ADACOM and provided in the following documents:

- ADACOM Certification Practice Statement for Qualified Electronic Signatures and Seals; and
- ADACOM Time Stamping Authority Certificate Policy & Certification Practices Statement

and described in a supplemental and simplified way in:

- PKI Disclosure Statement (PDS) for Qualified Electronic Signatures and Qualified Electronic Seals; and
- ADACOM Time Stamping Authority Disclosure Statement.

1.1 The Terms and Conditions govern Subscribers' use of Qualified Certificates for Electronic Signatures, Seals and Time Stamping Services and constitute a legally binding contract between Subscriber and ADACOM.

1.2 The Subscriber has to be familiar with and accept the current Terms and Conditions.

1.3 ADACOM reserves the right, at its sole discretion, to amend the Terms and Conditions at any time and without notice, should ADACOM have a justified need for such amendments. The current version and previous versions are published on: https://pki.adacom.com/repository/en/terms-and-conditions/

1.4 The Subscriber can apply for:

- Qualified Certificate for Electronic Signature (issued on a QSCD to a natural person)
- Qualified Certificate for Electronic Signature (issued on a QSCD to a natural person associated with a legal person)
- Qualified Certificate for Electronic Seal (issued on a QSCD to a legal person
- Advanced Electronic Seal (without a QSCD) issued to a legal person
- Qualified certificate for eSeal compliant with ETSI TS 119 495 under PSD2 issued to a legal person.

1.5 Identity verification & Application for the issuance of a Certificate

1.5.1 Before the issuance of a Qualified Certificate, the Subscriber's identity is verified by ADACOM using one of the following methods:

a) by the physical presence of Subscriber;

b) remotely, by means of a Qualified Certificate for electronic signature or electronic seal, provided that it has been initially issued based on physical presence or remotely, using electronic identification means; or

c) by Remote ID verification using video conference.

1.5.2 Subscriber/Subject shall sign and submit to ADACOM's RA/LRA the respective Application Form, as well as proof of identity and other required documents, as specified in the Application Form. Acceptable identification documents are National ID Cards from countries within the EU and passports from any other country. Greek Armed forces ID Cards may also be accepted.

ADACOM may assign part or the whole identity verification process to a third party.

1.6 In case of Qualified Electronic Seals compliant with ETSI TS 119 495, the Subscriber shall additionally provide the authorization number of the Payment Service Provider (PSP) issued by the National Competent Authority (NCA) supervising the PSP, the role of the PSP the name of the NCA, as well as the abbreviated unique identifier of the NCA. Additional verification will be performed by ADACOM consisting of validation of the PSP authorization number or any other registration number provided against NCA/EBA registry and validation of the role of PSP against the NCA/EBA registry.

1.7 The Subscriber of Qualified Time Stamping Services can be a natural person or natural person associated with legal person, or a legal person, by entering into a relevant contract with ADACOM.

1.8 For Subscribers whose identity is verified through the Remote ID verification method, the terms and

conditions specified in paragraph 5.4 shall apply additionally. Remote ID verification shall be available and feasible, only when the circumstances during the identity verification process are satisfactory enough to provide accurate proof of the Subscriber's ID.

1.9 ADACOM may refuse the issuance of the Certificate at its sole discretion if identity validation using any of the methods specified in par. 1.5 is not successful.

1.10 The Subscriber must complete the certificate issuance process within one month from the date of submission of the Application Form for the issuance of a Qualified Certificate.

1.11 Subscriber shall be legally eligible to apply for a Qualified Trust Service.

1.12 Subscriber agrees to use a Qualified Signature Creation Device (QSCD), which will be provided by ADACOM. QSCD can either be local or remote. The Subscriber is solely responsible for the proper use of the QSCD.

1.13 Subscriber may require the non-publication of the certificate to ADACOM's Public Directory.

1.14 Subscriber is responsible for the payment of any fees for the offered trust service, as well as any compensation arising from the improper use of the Certificate.

2. Certificate Acceptance for Electronic Signature or Seal, Certificate Types

2.1 Upon submitting an application for a Certificate, the Subscriber confirms that he/she is familiar with and accepts the Terms and Conditions.
The following acts constitute Certificate acceptance for Qualified Electronic Signature and Qualified Electronic Seal:

- The issuance of the Certificate constitutes the Subscriber's acceptance of the Certificate
- Failure of the Subscriber to object to the Certificate or its content within 24 hours from downloading it, constitutes Certificate acceptance.

2.2 If the Certificate re-keying is performed the Subscriber confirms that he/she has read and agrees to the Terms and Conditions.

2.3 Certificate Type, Usage and Certification Policy applied for:

Certificate Type	Usage	Certificate Policy Applied and Published
Qualified Electronic Signatures compliant with eIDAS.	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign	ADACOM Certification Practice Statement for Qualified Electronic Signatures and Qualified Electronic Seals, published https://pki.adacom.com/cps ETSI EN 319 411-2 Policy: QCP-n-qscd
Qualified or Advanced Electronic Seals compliant with eIDAS and/or ETSI TS 119 495 under PSD2	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.	ADACOM Certification Practice Statement for Qualified Electronic Signatures and Qualified Electronic Seals, published https://pki.adacom.com/cps ETSI EN 319 411-2 Policies: • QCP-l • QCP-l-qscd ETSI TS 119 495

Qualified Certificates are either Long-lived or Short-lived. A Long-lived Certificate is valid for 1 to 3 years and Short-lived Certificate is valid from 24 to 72 hours and can be used for one transaction.

3. Prohibitions of use

3.1 The Subscriber's Certificates shall not be used outside of the limits and contexts specified in ADACOM CPS for Qualified Electronic Signatures and Seals or for unlawful purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of ADACOM. Indicatively, the use of Certificates is prohibited for any of the following purposes:

a) unlawful activity (including cyber-attacks and attempt to infringe the Certificate);
b) issuance of new Certificates and information regarding Certificate validity;
c) enabling other parties to use the Subscriber's Private Key;
d) enabling the Certificate issued for electronic signing to be used in an automated way;

e) using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).

3.2 The Time Stamping Services shall be used within the limits and contexts specified in the TSA Certificate Policy & Certification Practice Statement. Any unlawful use outside those limits is prohibited.

4. Reliance Limits

4.1 Reliance Limits for Qualified Certificates for Electronic Signatures and Seals

4.1.1 The information in the Certificates is correct. There are no errors or material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.

4.1.2 Certificates become valid as of the date specified in them. The validity of the Certificate expires on the date of expiry indicated in the Certificate or if the Certificate is revoked.

4.1.3 Audit logs are retained on-site for no less than two (2) months. Physical or digital archive records regarding Certificate applications, registration information and requests or applications for suspension, termination of suspension and revocation are retained for at least seven (7) years after the expiry of the relevant Certificate.

4.2 Reliance Limits for Time Stamps

4.2.1 Time Stamps become valid as of the date specified in them. The validity of the Time Stamp expires on the date of expiry indicated in the Time Stamp or if the TSU Certificate is revoked. ADACOM TSA ensures that the Time Stamp Unit's 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 when a Time Stamp Unit's key usage period expires, and that Time Stamp Unit's private keys or any part, including any copies are destroyed such that the private key cannot be retrieved. The Time Stamp Token generation system shall reject any attempt to issue a Time Stamp Token if the signing private key is expired or if the signing private key usage period is expired.

4.2.2 ADACOM has in place technical procedures to ensure that Time Stamp Tokens are issued securely and include the correct time. The ADACOM Time Stamping Authority ensures that its time is synchronised with UTC within the declared accuracy with multiple independent time sources. The TSTs are issued with an accuracy of ± one (1) second. ADACOM implements security controls preventing unauthorised operation, aimed at calibration of TSA time. ADACOM monitors that synchronization is maintained when a leap second occurs.

4.2.3 Time-Stamping Certificates are valid for ten (10) years but require re-keying every year. Therefore, logs and records for Time-Stamping are retained for one (1) year after the expiration of the Time Stamping Unit Certificate.

5. Subscriber's Rights and Obligations - Indemnity

5.1 The Subscriber has the right to submit an application for issuing a Certificate or request a Time Stamp, accepting the present Terms and Conditions and adhere to the requirements provided in ADACOM's Certification Practice Statement for Qualified Certificates for Electronic Signatures and Electronic Seals and Time Stamping Authority Certificate Policy & Certification Practice Statement respectively.

5.2 The Subscriber and/or Subject of Qualified Electronic Signatures or Seals shall:

1. be solely responsible for the maintenance of their Private Key;
2. be solely and fully responsible for any consequences of using their Certificates both during and after the validity of the Certificate;
3. be solely liable for any damage caused due to failure or undue performance of their obligations specified in the present Terms and Conditions and/or the laws European Union.
4. be aware that Electronic Signatures or Electronic Seals given on the basis of expired or revoked Certificates are invalid.
5. submit accurate, true and complete information in relation to the issuance of the Certificate;
6. submit the necessary identification documents to ADACOM as specified in the Application Form for Certificate Issuance, as well as follow the steps that ADACOM indicates for completing the registration process;
7. not continue with the Certificate issuance procedure, if the Subscriber is not legally eligible to do so;

8. ensure that Subscriber´s Private Key is used under his/her control and exercise reasonable care to avoid unauthorized use of it;
9. be responsible for the secrecy of the Private Keys when residing on a Local QSCD, as well as the authentication credentials accessing private keys (username, password, OTP) when residing on a Remote QSCD;
10. be responsible for the proper use of the mobile device on which the application for the generation of the OTP has been installed in order to generate and use the Qualified Certificate residing on a Remote QSCD. If the Subscriber loses or destroys or is unable to use the Qualified certificate for any other reason outside ADACOM's control, the Subscriber should contact ADACOM directly in order to request revocation of his/her Certificate;
11. use his/her Private Key and Certificate in accordance with present Terms and Conditions, including applicable agreements set out in Section 9, and the laws of Greece and European Union;
12. notify ADACOM of the correct information during a reasonable time, in case of a change in his/her personal details, or of the legal person's details and/or of the legal person's representative or of any other inaccuracy of the Certificate content;
13. immediately inform ADACOM of a possibility of unauthorised use of his/her Private Key or if his/her Private Key has been lost, stolen, potentially compromised or if control over his/her Private Key has been lost due to a compromise of authentication credentials (e.g. PIN, PUK, username, password, OTP) or other reasons and immediately revoke his/her Certificate;
14. be responsible of placing the timestamp when signing with their Qualified Certificate;
15. not continue using the Private Key if the Certificate has been revoked or the CA has been compromised.
16. in case of Certificates compliant with ETSI TS 119 495 under PSD2, the Subscriber shall request revocation, if the Payment Service Provider (PSP) authorization is revoked or role(s) is/are revoked. The Subscriber is hereby notified that the NCA may also request revocation of these Certificates according to applicable regulatory requirements.

5.3 The Subscriber of Time Stamping Services shall:
1. verify the signatures created by the ADACOM TSA on the TST (Verification whether the TSA signature on the TST is valid and Verification of the TSA certificate);
2. use secure cryptographic functions for time-stamping requests;
3. be aware that expired Time Stamps are invalid.

5.4 The following terms shall additionally apply to the Subscriber whose identity is verified using the Remote ID verification method:
1. The Subscriber shall follow the instructions exactly as per ADACOM's authorized employee who is conducting the validation process.
2. The Subscriber shall present the identification document(s) in good condition to the extent that their originality can be verified.
3. At the beginning of the video conference and before the initiation of the verification process, the Subscriber must provide their explicit consent regarding the use, recording and storage of the remote ID verification process, taking snapshots of the Subscriber's face, identification document and, possibly, other necessary material.
4. If any third person other than Subscriber/Subject appears in the remote ID verification process, the session shall be terminated, any data recorded will be erased and the process will be repeated provided that no third persons appear.
5. ADACOM's authorized employee will discontinue the Remote ID verification process immediately:
   a) when the identification document is not appropriate or causes doubt as to its authenticity and reliability; or
   b) when the Subscriber behaves inappropriately towards ADACOM's authorized employee, or there are indications that the Subscriber is under duress, psychological or mental disorder or substance abuse; in these cases, the process cannot be repeated and the Subscriber must choose one of the other identity verification methods specified in par. 1.5.
6. The Subscriber shall submit to ADACOM an electronic solemn declaration, in which they will state their personal information in detail and their intention to proceed with the issuance of a qualified certificate.

5.5 To the extent permitted by applicable law, Subscribers are required to indemnify ADACOM for:
1. Falsehood or misrepresentation of fact by the Subscriber on the Application for the issuance of a Certificate;
2. Failure by the Subscriber to disclose a material fact on the Application, if the misrepresentation or omission was made negligently or with intent to deceive any party;

3. The Subscriber's failure to protect the Subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key;
4. The Subscriber's use of a name that infringes the Intellectual Property rights of a third party.

6. ADACOM's Obligations

Without prejudice to Section 8, ADACOM shall provide the services in accordance with the ADACOM Certification Practice Statement for Qualified Electronic Signatures and Seals, ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement, as well as the relevant legislation.

7. Certificate Status Checking Obligations of Relying Parties

7.1 A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in the relevant CP and CPS. A Relying Part acknowledges that he/she has access to sufficient information to ensure that he/she can make an informed decision as to the extent to which he/she will chose to rely on the information in a Qualified Certificate. A RELYING PARTY IS RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A QUALIFIED CERTIFICATE.

7.2 A Relying Party acknowledges and agrees that his/her use of ADACOM's Repository and his/her reliance on any Qualified Certificate shall be governed by ADACOM's applicable CPS as amended from time to time. The applicable CPS is published on the Internet in the Repository at https://pki.adacom.com/repository and is available via Email by sending a request to: practices@adacom.com. Amendments to the applicable CPS are also published in ADACOM's Repository at https://pki.adacom.com/repository.

7.3 If not enough evidence is referenced on the Certificate of Electronic Signature, or Electronic Seal with regard to the validity of the Certificate, a Relying Party verifies the validity, suspension or revocation of the Qualified Certificate using current revocation status information on the basis of certificate validation services offered by ADACOM at the time of using the Certificate or affixing a Qualified Electronic Signature or Qualified Electronic Seal. A method by which a Relying Party may check Certificate status is by consulting the most recent Certificate Revocation List from the Certification Authority that issued the Certificate on which he/she wishes to rely.

7.4 A Relying Party should take into account all limitations stated within any Certificate issued by ADACOM and makes sure that the transaction to be accepted corresponds to the relevant CP and CPS.

7.4.1 Qualified Certificates shall be used only to the extent that use is consistent with applicable law. Qualified certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

7.4.2 Time stamps shall be used only to the extent that use is consistent with applicable law. Any limitations on usage of time stamps indicated by the ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement should be taken into account. Subscribers and Relying Parties shall verify the signatures created by the ADACOM TSA on the TST. If the verification takes place after the end of the validity period of the Certificate, they should follow the guidance denoted in Annex D of ETSI EN 319 421.

7.5 ADACOM ensures the availability of its Trust Services 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.4% annually.

7.6 A Relying Party verifies the validity of any Certificate issued by ADACOM by checking OCSP and CRL references located in the Certificate.

7.7 Relying parties are expected to use a Trusted List to establish whether an Electronic Signature, Seal or Time Stamp is qualified.

8. Limited Warranty and Disclaimer/Limitation of Liability

8.1 ADACOM is liable for the performance of its Trust Services as specified in its Certification Practice Statement for the Use of Qualified Electronic Signatures and Seals and ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement.

8.2 ADACOM ensures that it has compulsory insurance contracts covering all ADACOM trust services to ensure compensation for damages caused by ADACOM's breach of obligations;

8.3 ADACOM informs all Subscribers and Subjects before ADACOM terminates service of Certificates and maintains the documentation related to the terminated service of Certificates and information needed according to the process set out in the CPS.

8.4 ADACOM is not liable for:

a) the secrecy of the Private Keys of Subscriber and Subject when residing on a local QSCD, or for possible loss or damage of the local QSCD;
b) the secrecy of the credentials accessing private keys (username, password, OTP) when residing on a remote QSCD, for possible loss or damage of the mobile device used for the OTP generation;
c) the improper use of a Certificate by the Subscriber/Subject or any misuse of the Certificate or inadequate checks of the Certificate or for the wrong decisions of a Subscriber/Subject or Relying Party or any consequences due to error or omission by the Subscriber/Subject or error or omission in Certificate validity checks;
d) forged electronic signature or electronic seal on a document, indicatively due to a stolen or compromised Private key or QSCD or otherwise.
e) the loss, improper storage, or improper use of time stamp tools;
f) the non-performance of its obligations if such non-performance is due to faults or security problems of the supervisory body, Trusted List or any other public authority;
g) the operation of software or other applications provided by third parties not related to ADACOM.
h) the failure to perform if such failure is occasioned by force majeure.

8.5 As stated in the respective CPS, ADACOM provides limited warranties and disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability, and excludes all liability, except in case of willful misconduct or gross negligence, for any loss of profits, loss of data, or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, performance, nonperformance, or compromise of certificates for electronic signatures, electronic seals, time stamps or any other transactions or services offered or contemplated herein, even if ADACOM has been advised of the possibility of such damages. In no event will the aggregate liability of ADACOM to all parties (including you) exceed the applicable liability cap for such qualified certificate set forth, below:

a) the combined aggregate liability of ADACOM to any and all persons concerning a specific qualified certificate shall be limited to an amount not exceeding five hundred (500) euro per certificate and a total maximum of claims of five hundred thousand (500,000) euro, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The liability limitations provided in this paragraph shall be the same irrespective of the number of certificates for Qualified Signatures/Seals, transactions, or claims related to such certificate.
b) the combined aggregate liability of ADACOM to any and all persons concerning Time Stamp Services shall be limited to an amount not exceeding that of the respective contract for the time stamping service, which will be calculated on a pro rata basis, and a total maximum of claims of five hundred thousand (500,000) euro, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The liability limitations provided in this paragraph shall be the same irrespective to the number of Time Stamps or claims related to such Time Stamp.

The limitations on liability provided herein shall apply to the maximum extent allowed under the applicable law of the applicable jurisdiction.

8.6 Subscribers, Subjects and Relying Parties are hereby notified of the possibility of theft or other form of compromise of a private key corresponding to a public key contained in a qualified certificate, which may or may not be detected, and of the possibility of use of a stolen or compromised key to forge a qualified electronic signature or qualified electronic seal on a document.

8.7 ADACOM may discontinue the validation process if any information provided by the Subscriber is found or suspected to be inaccurate or false or if identity verification of the Subscriber is not successful. Without prejudice to par. 8.5, ADACOM is not in any way liable for the authenticity or reliability of the identification documents submitted by the Subscriber nor for any damage that may be caused therefrom to the Subscriber or other persons.

8.8 Subscriber/Subject is hereby notified that, depending on the Subscriber/Subject's decision, ADACOM may use the following identifiers within the Certificate:

- Identification Card Number;
- Tax Identification Number;
- Unique Identifier.

One of the above identifiers shall be visible in Subscriber/Subject's electronic signature; ADACOM is not liable for any use thereof by third parties concerning the Subscriber/Subject's identity verification or identification or other uses thereof.

9. Applicable Agreements, Policies, CP, CPS

Relevant agreements, policies and practice statements related to the present Terms and Conditions are:

1. DigiCert Certificate Policy;
2. ADACOM Certification Practice Statement, for Qualified Certificates for Electronic Signatures and Electronic Seals;
3. Certificate and OCSP Profiles for Qualified Electronic Signatures and Qualified Electronic Seals and specifically:
   - Policy for Class 2 Certificate: Symantec/pki/policies/stn-cp/class2 (2.16.840.1.113733.1.7.23.2)
   - Policy for Qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD (0.4.0.194112.1.2)
   - Policy for Qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (0.4.0.194112.1.3)
   - Policy for Qualified certificate issued to a legal person where the private key and the related certificate do not reside on a QSCD (0.4.0.194112.1.1)
   - Normalized Certificate Policy (OID 0.4.0.2042.1.1)
   - Normalized Certificate Policy requiring a secure cryptographic device (OID 0.4.0.2042.1.2)
4. ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement
5. ADACOM Privacy Statement for the Protection of Personal Data
6. Current versions of all above applicable documents are published in ADACOM's repository at https://pki.adacom.com/repository

10. Privacy Policy and Confidentiality

10.1 ADACOM processes personal data according to the Privacy Statement, provided in the ADACOM's repository at https://pki.adacom.com/repository and all legal acts of European Union.

10.2 All information that has become known while providing services and that is not intended for disclosure (e.g. information that had been known to ADACOM because of operating and providing Trust Services) is confidential. The Subscriber has the right to obtain information from ADACOM about him/herself pursuant to the law.

10.3 ADACOM secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

10.4 ADACOM has the right to disclose information about the Subscriber or Subject to a third party who pursuant to relevant laws and legal acts is entitled to receive such information.

10.5 Additionally, non-personalized statistical data about ADACOM's services is also considered public information. ADACOM may publish non-personalized statistical data about its services.

11. Refund Policy

11.1 In case the sale of the Certificate is effected via the internet or a phone call the Subscriber has the right, under Article 3e of L. 2251/1994, as amended, to withdraw from the sales contract without stating the reasons within an exclusive time limit of fourteen (14) calendar days from the date of purchase. The exercise of this right shall be made in writing by the Subscriber to ADACOM, sending an email to qc@adacom.com. Subsequently, and following communication, ADACOM is obliged within fourteen (14) calendar days to repay the money corresponding to the value of the sales contract to the Subscriber, with the same means as those used for the initial transaction. Following that, the Subscriber is not entitled to use the Certificate. After that period, the right of withdrawal expires and ADACOM has no further obligation for the above cause.

11.2 Subject to section 11.1, ADACOM handles refunds on a case-by-case basis.

12. Applicable law, complaints and dispute resolution

12.1 Any disputes related to the trust services provided under these terms shall be governed in all respects by and construed in accordance with the laws of Greece excluding its conflict of laws rules, and European Union as the location where ADACOM is registered as a CA. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

12.2 To the extent permitted by law, before any dispute resolution mechanism may be invoked with respect to

a dispute involving any aspect of ADACOM's trust services, the Subscriber or other party must notify ADACOM, and any other party to the dispute of any claim or complaint not later than thirty (30) calendar days after the detection of the basis of the claim, unless otherwise provided by law. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may seek legal resolution. All parties agree that the courts of Athens, Greece, shall have exclusive jurisdiction and venue for hearing and resolving any dispute regarding the interpretation and execution of these terms and the provision of ADACOM's services.

12.3 The Subscriber or other party can submit their claim or complaint on the following email: practices@adacom.com

12.4 All dispute requests should be sent to contact information provided in these Terms and Conditions.

13. ADACOM and Repository Licenses, Trust Marks and Audit

13.1 ADACOM S.A. is a Qualified Trust Service Provider and is granted the qualified status by a supervisory body and is listed in the EU Trusted List for Certification Service Providers, following the submission of a conformity assessment report by an accredited Conformity Assessment Body.

13.2 ADACOM's Trusted Services are registered in the EU Member States Trusted List which includes information related to the qualified trust service providers which are supervised by the competent Member State, available at:
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
The prerequisite requirement of this registration is in compliance with Regulation (EU) No 910/2014.

13.3 The Conformity Assessment Body which audits ADACOM is accredited in accordance with Regulation (EC) No 765/2008 as competent to carry out conformity assessment of Qualified Trust Service Providers.

13.4 Audit conclusions or certificates, which are based on audit results of the conformity assessment conducted pursuant to the eIDAS Regulation, corresponding legislation and standards are published on ADACOM's website https://pki.adacom.com/repository .

14. Contact Information

14.1 Qualified Trust Service Provider
ADACOM S.A.
Kreontos 25 Str
104 42 Athens, Greece
http://www.adacom.com
Phone +.30 210 5193750
Fax +30 210 5193555
E-mail: practices@adacom.com

14.2 The applications for revoking Certificates are accepted from 09:00 to 19:00 (UTC+2) via phone at +30 210 9577255, via email at revoke@adacom.com, or via self-service web portal.

14.3 Website Information and contact details of the self-service web portal is available on https://pki.adacom.com/repository.

15. Validity of Terms and Conditions

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

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