ADACOM

SECURITY BUILT ON TRUST

Terms and Conditions for Qualified Trust Services (Electronic Signatures, Seals and Time Stamps)

version 6.3

ADACOM S.A. Commercial reg. no: 3537101000

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)
15.11.2021	5.0	Major changes and complete text reformation
31.01.2022	5.1	Change in par. 14.5 (h)
10.02.2023	6.0	Changes in par. 4.2, 5.9, 16.1
22.01.2024	6.1	Minor change in par. 14.7
8.10.2024	6.2	Changes in par. 4.1 (c), section 5, par. 19.2: Removal of teleconference with agent from Remote Identity Proofing, Insertion of eIDAS amending Regulation.
30.03.2026	6.3	Changes in par. 4.2

THESE TERMS AND CONDITIONS AFFECT YOUR LEGAL RIGHTS. PLEASE READ THEM CAREFULLY. BY ACCEPTING THESE TERMS AND CONDITIONS, YOU AGREE TO FOLLOW AND BE BOUND BY THEM.

1. General Terms

1.1 The present Terms and Conditions for Qualified Trust Services (hereafter "Terms and Conditions") govern the use of Qualified Certificates for Electronic Signatures, Seals and Time Stamps by Subscriber (hereafter "Subscriber") and constitute a legally binding agreement between Subscriber and ADACOM Qualified Trust Service Provider (hereafter "ADACOM").

1.2 Subscriber shall be familiar with and accept the Terms and Conditions as applicable from time to time.

1.3 ADACOM reserves the right to amend the present Terms and Conditions at any time and without notice, if there is a justified need for such amendment. The current version and previous versions are published on ADACOM's Repository

1.4 ADACOM may refuse the issuance of the Certificate at its sole discretion if Subscriber's identity verification is not successful.

1.5 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.

1.6 Subscriber shall be legally eligible or duly authorized to apply for the issuance of a Qualified Certificate or for any trust service in general.

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

1.8 Subscriber request the non-publication of the certificate on ADACOM's Public Directory.

1.9 Subscriber shall pay the fees for the offered trust service, as well as any compensation that may arise from the improper use of the Certificate or the trust service.

1.10 The Certificate may in no case be transferred to another person.

2. Trust Services

The Trust Services offered by ADACOM that Subscriber can apply for are the following:

- Qualified Certificate for Electronic Signature issued to a natural person, with the use of local or remote QSCD,
- Qualified Certificate for Electronic Signature issued to a natural person associated with a legal person, with the use of a local or remote QSCD,
- Qualified Certificate for Electronic Seal issued to a legal person, with the use of a local or remote QSCD,
- Advanced Electronic Seal issued to a legal person (without the use of a QSCD)
- Qualified Certificate for Electronic Seal to a legal person, compliant with ETSI TS 119 495 under PSD2 Directive (see Section 6),
- Qualified Time-Stamping (see Section 7).

Qualified Certificates for Electronic Signatures are either Long-term or Short-term. A Long-term Certificate is valid for 1 to 3 years and a Short-term Certificate is valid from 24 to 72 hours.

3. Reliance Limits

3.1 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.

3.2 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.

3.3 ADACOM maintains a record that includes all the information in relation to the Certificates it issues, i.e. Certificate applications, registration information, identity verification documents, requests for revocation etc., for at least seven (7) years after the expiry or revocation of the relevant Certificate. Audit logs are retained for no less than two (2) months. Physical or digital archive records regarding are retained for at least seven (7) years after the expiry of the relevant Certificate.

4. Identity Proofing & Certificate Application

4.1 Before the issuance of a Qualified Certificate, ADACOM verifies the Subscriber's identity by using one of the following methods:

a) by the physical presence of Subscriber; or

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

c) by Remote Identity proofing through an automated video which is later checked by ADACOM's agent who is responsible for verifying that the video is acceptable as per the regulatory requirements (hereafter "Remote Identity Proofing"). If the automated video call is unsuccessful for multiple times, then the person has the option to be verified by physical presence.

For more information, please refer to the section Identity Verification Methods on ADACOM's Repository.

4.2 Subscriber shall submit to ADACOM the relevant Certificate Application, as well as the necessary identification documents, as specified by ADACOM. Subscriber shall submit accurate, true and complete information. ADACOM shall accept original documents or copies which are drafted in the language of the Subscriber's jurisdiction either in hard copy or electronic form and which bear wet or electronic signatures or certification of signatures, as the case may be.

Please refer to the List of Acceptable ID documents on ADACOM's Repository.

ADACOM may assign identity proofing, partially or wholly, to a third party.

4.3 The Certificate Application is submitted through the ADACOM Portal. Upon submitting the Application for the issuance of a Certificate, Subscriber confirms that they have read and accept the Terms and Conditions.

4.4 For Subscribers who choose the use of Remote Identity Proofing, the terms specified in Section 5 shall additionally apply.

5. Remote Identity Proofing

5.1 Subscriber shall strictly follow the instructions indicated by ADACOM. Remote Identity Proofing shall be performed with sound and video quality that shall allow the verification of the natural person who is being identified ("Identified Person") with a satisfactory degree of certainty.

5.2 The identification document presented by Subscriber shall be original and in a condition that allows to verify its authenticity.

5.3 If the Identified Person presents the old type of Greek ID card which contains Latin characters, then they shall also submit to ADACOM an electronic solemn declaration through gov.gr, in which they will state their personal details and their intention to proceed with the issuance of a qualified certificate. This is not applicable for the new type of Greek ID cards which contain advanced security features.

5.4 During the Remote Identity Proofing process a video of the Identified Person shall be taken, as well as snapshots from both sides of the ID document containing their details.

5.5 To complete the Remote Identity Proofing, a unique One Time Password (OTP) will be sent from ADACOM to the Identified Person via SMS, which is automatically and randomly generated. The process will be considered complete only after the password is confirmed by the system.

5.6 The Identified Person shall provide their explicit and special consent regarding the collection, recording and retention of all data and files required for the Remote Identity Proofing.

5.7 Compulsory Termination

The Remote Identity Proofing process shall be terminated in the following cases:

a. When identity proofing is not feasible due to poor lighting, poor image and/or sound quality, interruptions in data transmission or interruptions in the flow of the procedure.

b. When the ID document is not suitable.

c. When there is doubt as to the validity and reliability of the ID document.

d. When there is doubt about other elements that are examined during the Remote Identity Proofing procedure.

e. When it is not possible to communicate with the Identified Person for reasons other than those mentioned in case a. above or when a third person, other than the Identified Person, appears during the procedure.

f. When there are indications that the Identified Person is under duress, psychological or mental disorder or substance abuse.

In cases c. and d. above, the remote identity proofing process must be terminated and may be conducted using an alternative method from those listed in Section 4.1. In all other cases, the process is interrupted and may be repeated from the beginning. In case b. the process may be repeated if an appropriate ID document is submitted.

5.8 Remote Identity Proofing is available in Greek and English. For more information, please refer to the section Remote Identity Proofing on ADACOM's Repository.

6. PSD2 Electronic Signatures

6.1 In accordance with ETSI TS 119 495, 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 verification of the PSP authorization number or any other registration number provided against NCA/EBA registry and verification of the role of PSP against the NCA/EBA registry.

6.2 Subscriber shall request revocation of the Certificate, if the PSP authorization is revoked or role(s) of the PSP is/are revoked. The NCA may also request the Certificate's revocation according to applicable regulatory requirements.

7. Electronic Time Stamps

7.1 Subscriber of Qualified Time-Stamping Services can be a natural person or legal person, by entering into a relevant agreement with ADACOM.

7.2 Subscriber shall be responsible for placing the Time Stamp when signing with their Qualified Certificate.

7.3 Reliance Limits for Time Stamps

7.3.1 Time Stamps become valid as of the date specified in them. Expired Time Stamps are invalid. The validity of the Time Stamp expires on the date of expiry indicated in the Time Stamp or if the Time-Stamping Unit (TSU) Certificate is revoked. ADACOM Time-Stamping Authority (TSA) ensures that the 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 when a TSU key usage period expires, and that TSU private keys or any part thereof, including any copies, are destroyed in such a way that the private key cannot be retrieved. The Time Stamp Token (TST) generation system shall reject any attempt to issue a TST if the signing private key has expired or if the signing private key usage period has expired.

7.3.2 ADACOM has in place technical procedures to ensure that TSTs are issued securely and include the correct time. ADACOM TSA ensures that its time is synchronized with the Coordinated Universal Time (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 that prevent unauthorized operation, aimed at calibration of TSA time. ADACOM monitors that synchronization is maintained when a leap second occurs.

7.3.3 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 TSU Certificate.

7.3.4 Subscriber of Time-Stamping Services shall:

a) use secure cryptographic functions for time-stamping requests;

b) verify that:

- the Time-Stamping Unit (TSU) Certificate belongs to ADACOM
- the TSU Certificate has not been revoked
- it is marked as qualified
- the issuing TSA Certificate has not been revoked.

7.3.5 Relying Parties of Time-Stamping Services shall verify that:

- the Time-Stamping Unit (TSU) Certificate belongs to ADACOM
- the TSU Certificate has not been revoked
- it is marked as qualified
- the issuing TSA Certificate has not been revoked.

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

8.1 The failure of the Subscriber to object to the Certificate or its content within 24 hours from downloading it constitutes Certificate acceptance by Subscriber.

8.2 Certificate Type and applicable Policy:

Certificate Type	Certificate Policy Applied and Published
Qualified Electronic Signatures compliant with eIDAS	ADACOM Certification Practice Statement for Qualified Electronic Signatures and Qualified Electronic Seals, published on https://pki.adacom.com/cps ETSI EN 319 411-2 Policy: QCP-n-qscd
Qualified Electronic Seals compliant with eIDAS	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
Advanced Electronic Seals compliant with ETSI TS 119 495 under PSD2	ADACOM Certification Practice Statement for Qualified Electronic Signatures and Qualified Electronic Seals, published https://pki.adacom.com ETSI TS 119 495 Policies
Qualified Time-Stamping	Qualified Time Stamping Authority Certificate Policy & Certification Practice Statement ETSI EN 319 421, ETSI EN 319 422 Policies

9. Acceptable use

9.1 A qualified electronic signature has equivalent legal effect of a handwritten signature and is linked to the signatory so that the latter cannot deny in the future that he was the one who signed.

9.2 A qualified electronic seal is used to ensure the origin and integrity of the data to which it is linked.

9.3 Certificates shall not be used outside the limits and contexts specified in ADACOM Certification Practice Statement or for unlawful purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of ADACOM.

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

10. ADACOM's Obligations

Without prejudice to Section 14, ADACOM shall provide the trust services in accordance with the ADACOM Certification Practice Statement, as well as the relevant legal and regulatory framework for Trust Service Providers.

11. Subscriber's Obligations

Subscriber and/or Subject of a Qualified Certificate for Electronic Signature or Electronic Seal shall:

a) use his Private Key and Certificate in accordance with present Terms and Conditions, including applicable agreements set out in Section 15, and the laws of Greece and European Union;

b) ensure that his Private Key is used under his control and exercise reasonable care to avoid unauthorized use thereof;

c) be responsible for the maintenance and ensuring the secrecy of his Private Key when his

Certificate is issued on Local QSCD, whereas he shall be responsible for the credentials (username, password, OTP) accessing the Private Key when his Certificate is issued on a Remote QSCD.

d) be solely and fully responsible for any consequences from using his Certificate during and after the Certificate's validity;

e) be solely liable for any damage caused due to failure or undue performance of his obligations specified in the present Terms and Conditions and/or the law.

f) be aware that Electronic Signatures or Electronic Seals issued based on expired or revoked Certificates are invalid.

g) be responsible for the proper use of the mobile device which was used for the installation of the application to generate the OTP in order to issue the Qualified Certificate on a Remote QSCD. If the Subscriber's device is lost or destroyed or Subscriber is unable to use his Certificate for any other reason outside ADACOM's control, Subscriber shall contact ADACOM immediately in order to request revocation of his Certificate.

h) immediately inform ADACOM in case of theft, loss or unauthorised use of his Private Key or his credentials (e.g. password, OTP) and immediately revoke his Certificate;

i) discontinue using his Certificate if it has been revoked.

j) In case of a change in his personal details, or the legal person's details or the details of the legal person's representative or in case of any other inaccuracy in the Certificate's content, Subscriber shall notify ADACOM of the correct information within a reasonable time.

12. Relying Parties Obligations

12.1 Any Relying Party studies the risks and liabilities related to the acceptance of a Certificate. A Relying Part acknowledges that he has access to sufficient information to ensure that he can make an informed decision as to the extent to which he will chose to rely on the information in a Certificate. A Relying Party is responsible for deciding whether or not to rely on the information in a Certificate.

12.2 A Relying Party acknowledges and agrees that his use of ADACOM's Repository and his reliance on any Certificate shall be governed by ADACOM's Certification Practice Statement, as applicable at any time.

12.3 If not enough evidence is referenced in the Certificate regarding its the validity, a Relying Party shall verify the validity, suspension or revocation of the Certificate using current revocation status information based on the most recent Certificate Revocation List of the ADACOM Certification Authority.

12.4 Any limitations on usage of time stamps indicated by the ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement should be taken into account

12.5 A Relying Party shall verify the validity of any Certificate issued by ADACOM by checking OCSP and CRL references located in the Certificate.

12.6 A Relying Party is expected to use a Trusted List to establish whether an Electronic Signature, Seal or Time Stamp is qualified.

13. Certificate Revocation

13.1 Subscriber may request the revocation of a Certificate at any time by contacting ADACOM as provided in paragraph 20.2. ADACOM also has the right to revoke a Certificate only in the cases listed below. The revoked Certificate is published in the Certificate Revocation List (CRL).

13.2 A Certificate me by revoked by ADACOM in the following cases:

i. ADACOM believes or strongly suspects that the Certificate has been compromised;
ii. ADACOM has reason to believe that the Subscriber has breached a material obligation under the present Terms and Conditions;
iii. ADACOM has reason to believe that the Certificate was issued in a manner not in accordance with its applicable procedures or issued to a person other than the one named in the Application or a that an unauthorized person has requested the issuance of the Certificate;

iv. ADACOM has reason to believe that a material fact in the Certificate Application is inaccurate or false, or becomes aware of changes which impact the validity of the certificate;
v. Subscriber loses his legal eligibility, passes away, is declared absent; or is under liquidation or other similar procedure;
vi. Subscriber loses ability to use the local QSCD or mobile device required to access a remote QSCD;
vii. Subscriber requests revocation of the Certificate of a natural person associated with a legal person.
viii. A final court judgment requires the revocation;
ix. The private key of the CA has been compromised. In this case ADACOM will make a relevant announcement
x. The Supervisory Body requests the revocation;
xi. Subscriber has not submitted payment, when due;
xii. Continuing the use of a certificate is harmful to ADACOM.

14. Warranties – Limitations of Liability – Indemnity

14.1 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

14.2 ADACOM is liable for the performance of its trust services as specified in its applicable Certification Practice Statement.

14.3 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

14.4 ADACOM informs all Subscribers, Subjects, the supervisory body and other parties with which it maintains relevant agreements and which may be affected, before it terminates any trust service and maintains documentation related to the terminated service, as well as the information necessary according to legal requirements.

14.5 Disclaimer.

ADACOM is not liable for:

a) the secrecy of the Subscriber and Subject's Private Keys when residing on a local QSCD, or for loss or damage of the local QSCD;
b) the secrecy of the credentials accessing Private Keys (e.g. Username, Password, OTP) when residing on a remote QSCD, for loss or damage of the mobile device used for the OTP generation;
c) incorrect, improper use or misuse of a Certificate by the Subscriber/Subject or inadequate checks of the Certificate or for the incorrect decisions of a Relying Party to rely on a Certificate or any consequences due to error or omission by the Subscriber, Subject or Relying Party during the Certificate validity check;
d) the placement of any unauthorized electronic signature or electronic seal on documents, indicatively due to a stolen or unauthorized use of a 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 of the Trusted List or delays or omissions of the supervisory body or any other authority;
g) the operation of software or other applications provided by third parties not related to ADACOM;
h) the non-authenticity of identification documents or for any damage caused to the Subscriber or other persons for this reason provided that the procedure set out in ADACOM's identity verification policy has been followed and that all required checks have been performed during the verification of the document's authenticity;
i) the failure to perform if such failure is due to force majeure;
j) Depending on the Subscriber/Subject's decision, ADACOM may use the ID Card Number, the Tax Identification Number or a Unique Identifier, one of which shall be included in the Certificate; ADACOM is not liable for any use of the above identifiers by third parties outside ADACOM's control.

14.6 Limitations of liability.

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, or consequential damages arising from 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.

14.6.2 In no event shall the aggregate liability of ADACOM to all parties exceed the maximum liability cap as set forth, below:

a) The 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 for all claim, regardless of the nature of the liability and the type, amount or extent of the damages. The liability limitations provided in this paragraph shall be the same irrespective of the number of Certificates, transactions, or claims related to such Certificate.
b) The aggregate liability of ADACOM to any and all persons concerning Time-Stamping Services shall be limited to an amount not exceeding that of the respective agreement for the time-stamping service, 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 the damages. 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.

14.7 Indemnity

To the extent permitted by applicable law, and provided ADACOM suffered any damages therefrom, Subscribers are required to indemnify ADACOM for:

a) inaccuracies or misrepresentations of information on the Certificate Application; or Subscriber's failure to disclose important information which will affect the Certificate's content, if such false representation or omission made with intent to deceive any party;
b) Subscriber's failure to protect his private key, to use a trustworthy system, or to otherwise take the preventive measures necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of his private key;
c) the Subscriber's use of a name that infringes the Intellectual Property rights of any third party.

15. Applicable Agreements, Policies, CP, CPS

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

1. ADACOM Certification Practice Statement for Qualified Certificates for Electronic Signatures and Electronic Seals;
2. 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)
3. ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement
4. ADACOM Privacy Statement

Current versions of all above applicable documents are published on the ADACOM Repository.

16. Privacy Policy and Confidentiality

16.1 ADACOM processes personal data according to the Privacy Statement, which is published on the ADACOM Repository according to the applicable national and European legal framework for the protection of personal data, i.e. the General Data Protection Regulation (GDPR).

16.2 All information that has become known while providing services and that is not intended for disclosure (e.g. information that ADACOM has become aware of from operating and providing Trust Services) is confidential. Subscriber and Subject have the right to be informed about the information that ADACOM maintains for them, pursuant to the law.

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

16.4 ADACOM has the right to disclose information about Subscriber or Subject to third parties who pursuant to relevant legislation are entitled to receive such information.

16.5 Additionally, ADACOM may publish non-personalized statistical data about its services.

17. Refund Policy

17.1 In case the sale of the Certificate is effected via the internet or telephone, 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, by sending an email to qc@adacom.com. Subsequently, and following communication, ADACOM is obliged within fourteen (14) calendar days to refund the amount corresponding to the sales contract to the Subscriber, through the same payment method used for the initial transaction. Following this refund, Subscriber is not entitled to use his Certificate. After that period, the right of withdrawal expires and ADACOM has no further obligation for the above cause.

17.2 Subject to the above paragraph, ADACOM handles refunds on a case-by-case basis.

18. Applicable law, complaints and dispute resolution

18.1 Any disputes related to the trust services provided under these Terms and Conditions shall be governed and construed in accordance with the laws of Greece. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

18.2 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 any other interested 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 the interested party may seek court resolution. All parties agree that the courts of Athens, Greece, shall have exclusive jurisdiction and are competent to resolve any dispute regarding the interpretation and application of these Terms and the provision of ADACOM's services.

18.3 The Subscriber or other party may submit their claim or complaint in the following email: practices@adacom.com.

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

19. Licenses, Trusted List and Audit

19.1 ADACOM is a Qualified Trust Service Provider and its Trust services are registered in the national EETT Registry of Providers and the EU Trusted List.

19.2 ADACOM is subject to regular audits by a Conformity Assessment Body which certifies the services according to Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 (eIDAS Regulation).

19.3 Certifications which are based on audit results of the conformity assessment audit conducted

pursuant to the eIDAS Regulation, the corresponding legislation and standards are published on the ADACOM Repository.

20. Contact Information

20.1 ADACOM S.A.
25 Kreontos Str.
10442 Athens, Greece
http://www.adacom.com
Tel: +.30 210 5193740
E-mail: practices@adacom.com

20.2 The applications for Certificate revocation are accepted via email at revoke@adacom.com, or the ADACOM Portal or telephone at +30 210 9577255 from 09:00 to 19:00 (UTC+2).

21. Validity of Terms and Conditions

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

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

22. Definitions and Acronyms

Term/Acronym	Definition
Automated video	Asynchronous video with final human decision, a process of remote identity proofing through an information system that allows the registration and collection of identity proofing data of a natural person, the uploading of electronic documents, the recording of image and sound (video) in order to verify the liveliness of the natural person, without the presence of an operator of the TSP, but with the final decision taken by the person conducting the identity proofing after examining all the data.
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, as amended by Regulation (EU)

	2024/1183 of the European Parliament and of the Council of 11 April 2024.
EBA	European Banking Authority
Identified person	The natural person who acts for himself individually or as a legal representative of a legal person or entity.
Identity proofing/ Identity verification	The process by which a trust service provider collects and validates information about an applicant Subscriber and verifies that collected and validated information actually belongs to the applicant.
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-term 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 or 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 the eIDAS Regulation.
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 Qualified Signature/Seal Creation Device that meets the requirements of Art. 30 of the eIDAS Regulation. A QSCD can be either local in the form of a USB token/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 Identity proofing	The method/process by which a natural person is identified through an automated video and is equivalent to identity verification through physical presence.
Short-term Certificate	A Qualified Certificate which is valid from 24 to 72 hours.
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.
Terms and Conditions for Qualified Trust Services	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.
TSP	Trust Service Provider
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	A list containing information about qualified trust service providers in the EU, as well as information on the qualified trust services provided by them.

ADACOM

SECURITY BUILT ON TRUST

GREECE / HQ

25 Kreontos str.
104 42 Athens
+30 210 51 93 740

GREECE / Thessaloniki Office

8 Chalkis str.
555 35 Pylaia Thessaloniki
+30 2310 365 25

CYPRUS

10, Katsoni str. 1082,
Nicosia
+357 22 444 071

UNITED KINDOM

88 Wood St., Barbican EC2V 7RS,
London
+44 (0) 203 126 4590

KINGDOM OF BAHRAIN

Manama Center, Blog: 316
Road: 383, Building: 128
Flat/Office: 2030