ADACOM

SECURITY
BUILT ON TRUST

ADACOM

PKI Disclosure Statement

Effective Date: 10 February 2023

Version 5.0

ADACOM S.A. Commercial reg. no: 3537101000

Version History		
Date	Version	Changes
18.05.2018	1.0	Initial document
10.01.2019	1.1	Minor changes in Section 4
25.02.2019	1.2	Minor changes in Section 5
25.06.2019	1.3	Minor changes in Sections 1 and 5
01.04.2020	1.4	Minor changes in Sections 5 and 8
10.05.2020	2.0	Addition of validation methods in Section 5
17.02.2021	3.0	Addition of section 3, minor changes in Section 4, 5, 6, 9, 10, 11, 12
22.02.2022	4.0	Major changes in all sections and renumbering
10.02.2023	5.0	Change in section 4

Table of Acronyms	
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
LRA	Local Registration Authority
OCSP	Online Certificate Status Protocol
QSCD	Qualified Signature Creation Device
RA	Registration Authority

1. Overview

This document aims to provide summarized information to the Subscriber and Relying Parties about Qualified Certificates and trust services provided by ADACOM which are governed by ADACOM Certification Practice Statement ("CPS") and the Terms and Conditions for Qualified Trust Services ("Terms and Conditions").

This document does not substitute or replace ADACOM's Terms and Conditions nor the CPS; it only summarizes the key points for the benefit of Subscribers and Relying Parties.

2. Contact info

ADACOM S.A.
Qualified Trust Service Provider
25, Kreontos Street,
104 42 Athens, Greece
http://www.adacom.com
E-mail: practices@adacom.com
Telephone +.30 210 51 93 740
(Mon-Fri 09.00. – 19:00, UTC+02:00)

3. Important information

- Subscriber shall be aware of and accept ADACOM's applicable Terms and Conditions.
- Subscriber must complete the certificate issuance process within one month from the date of submission of the Certificate Application.
- Subscriber shall be legally eligible or duly authorized to submit the Certificate Application.
- Subscriber agrees to use the Qualified Signature Creation Device (QSCD) which will be provided by ADACOM. The QSCD can either be local or remote. Subscriber is solely responsible for the proper use of the QSCD.
- Subscriber may require the non-publication of the certificate to ADACOM's Public Directory.
- 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 or the trust service.
- ADACOM is not liable for the operation of software or other applications provided by third parties outside ADACOM's control.

4. Certificates types, Identity proofing procedures and Use

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,
- Qualified Time-Stamping.

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.

The Subscriber's identity is verified 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; or
c) by remote identity proofing.

A natural person's identity in verified by providing proof of his/her identity.
A legal person's identity is verified through its legal or authorized representative.

Subscriber shall provide the necessary documents specified by ADACOM.

Subscriber shall submit to ADACOM the relevant Certificate Application which constitutes a binding agreement between Subscriber and ADACOM, as well as the necessary identification documents as the case may be. Subscriber shall submit accurate, true and complete information. ADACOM shall accept original documents or certified copies according to the rules applicable to Subscriber's jurisdiction, which are drawn up in Greek, English, French or German; if they are drawn up in any other language, translations in one of the above languages shall be accepted.

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

Available identity verification methods can be found here.

The list of acceptable identification documents can be found here.

For more information about remote identity proofing you can consult the instructions available here.

Certificate shall be used as prescribed by the CPS and Terms and Conditions only. Any different usage is forbidden.

5. Revocation

Subscriber may request revocation of the Certificate via email at revoke@adacom.com, or via telephone at +30 210 9577255, or alternatively via ADACOM's Portal. ADACOM will promptly initiate revocation of the certificate.

6. Subscriber's Obligations

The certificate subscriber has the obligations set forth in the CPS and the Terms & Conditions. In particular, but not only, Subscriber has the following obligations:

- Provide ADACOM with precise, true and complete information in Certificate Applications;
- Use the Certificate only in the ways and for the purposes provided for in the CPS;
- Protect and ensure the safety of his local QSCD or his credentials in case of remote QSCD;
- Not leave his local QSCD or his authentication credentials in case of remote QSCD exposed and always place them in a secure location;
- In the event of loss, theft or destruction of his private key, immediately contact ADACOM.

7. Relying parties' obligations

Relying Parties shall check the status of Certificates on which they wish to rely. A way of checking the Certificate's current status is by consulting the most recent Certificate Revocation List (CRL) from ADACOM CA that issued the Certificate.

Alternatively, Relying Parties may check the Certificate status using the ADACOM's online repository or OCSP responder. ADACOM provides Relying Parties with information on how to find the appropriate CRL, Repository or OCSP responder to check whether Certificates have been revoked.

8. Reliance Limits

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.

9. Applicable Agreements, CP, CPS

Relevant agreements, policies and practice statements for use of Certificates are:

- ADACOM Certificate Policy and Certification Practice Statement for Qualified Certificates for Electronic Signatures and Electronic Seals
- ADACOM Terms & Conditions for Qualified Trust Services
- Certificate and OCSP Profiles for Qualified Electronic Signatures and Qualified Electronic Seals

Current versions of all applicable documents are publicly available in ADACOM's repository at https://pki.adacom.com/repository

10. Refund Policy

ADACOM makes efforts to secure the highest level of quality of its services.
In case the sale of the Certificate is effected via the internet or telephone the Subscriber has the right to withdraw from the purchase. Subscriber shall exercise this right in writing by sending an email to qc@adacom.com.

11. Privacy Policy

ADACOM processes personal data in accordance to applicable data protection legislation.

For further details, please refer to ADACOM's Privacy Statement at https://pki.adacom.com/repository

12. Licenses, Trusted List and Audit

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.

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

13. Limited warranty and Disclaimer, Limitation of liability

For warranty and liability limitations, please refer to the Terms and Conditions published on ADACOM's Repository.

14. Applicable Law, Complaints, Dispute Resolution

Any disputes related to the trust services provided by ADACOM shall be governed by the laws of Greece. Subscriber must notify ADACOM 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 Subscriber may seek court resolution. The Courts of Athens, Greece, shall have exclusive jurisdiction and competence to resolve any dispute related to ADACOM's trust services.