ADACOM
Qualified Time Stamping Authority Certificate Policy & Certification Practice Statement

Version 1.2

Effective Date: 15/02/2019

ADACOM S.A.
25 Kreontos Street
10442 Athens
Greece
Phone number: +30 210 5193740
https://www.adacom.com

© 2019 ADACOM S.A. All rights reserved.

Document Information

The present document has been developed by ADACOM S.A. and contains the conditions, according to which ADACOM is acting as a Qualified Time Stamping Service Provider (QTSSP)

The present document is based on and thus compatible with the Standard EN 319 421 “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”

Intellectual Property Rights

Copyright in this document belongs to ADACOM. All rights reserved. Except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of ADACOM S.A.

Requests for any other permission to reproduce this publication (as well as requests for copies from ADACOM S.A.) must be addressed to ADACOM S.A., 25 Kreontos street, 10442, Sepolia, Greece Attn: Policy Management Authority. Tel: +30 210 5193750, Fax: +30 210 5193555, Email: practices@adacom.com.

Version History

Date	Version	Changes
10/01/2019	1.0	Initial document
25/01/2019	1.1	Minor changes in par. 7.4.7
15/02/2019	1.2	Minor changes in par. 4.2

Contents

1. Introduction

This document constitutes ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement for Qualified Time Stamping Services. It is intended to describe the rules and operational procedures adopted by ADACOM who is a Qualified Trusted Service Provider (QTSP) for the provision of Qualified Time Stamping Services according to Regulation (EU) N° 910/2014 [eIDAS].

ADACOM's Qualified Time Stamping Services support assertions of proofs that an electronic record existed before a particular time. These services can be used in support to non-repudiation services, to prove that an electronic signature was generated during the validity period of a public key certificate, to support electronic long term archiving, etc.

The ADACOM Qualified Time Stamping Services is a part of ADACOM's PKI services.

The current document specifies general rules used by the ADACOM Time Stamping Authority (TSA) for the issuance of Time Stamp Tokens (TST). It defines the parties involved, their responsibilities, rights and the applicability range.

The ADACOM Time Stamping Services can be reached via https://tss.adacom.com/qtss

The Time Stamping Authority does no long-term archiving of any timestamp token and the application using the TSA must save the issued token for a future usage.

The ADACOM Qualified Time Stamping Services are provided according to eIDAS regulation, to the EN 319 421 and to EN 319 422 standards and under the authority of ADACOM acting as Qualified Time Stamping Services Provider.

Management may make exceptions to this CP/CPS on a case-by-case basis to mitigate material, imminent impacts to customers, partners, relying parties, and/or others where practical workarounds do not exist. Any such management exceptions are documented, tracked, and reported as part of the audit process.

1.1 Policy Administration

Organization Administering the Document
ADACOM S.A.
25, Kreontos Street
10442, Athens
Greece

Contact Person
PKI Policy Manager
ADACOM Policy Management Authority
c/o ADACOM SA
25, Kreontos Street,
10442, Athens,
Greece
phone number +30 210 5193750
fax number: +30 210 5193555
practices@adacom.com

1.2 Approval Procedure

Approval of this CP/CPS and subsequent amendments are made by the PMA. Amendments are either in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be linked to the ADACOM Repository located at: https://pki.adacom.com/repository.

Updates supersede any designated or conflicting provisions of the referenced version of the CP/CPS. The PMA shall determine whether changes to the CP/CPS require a change in the Certificate policy object identifiers of the Certificate policies.

2. References

The following documents contain provisions which are relevant to the ADACOM Qualified Time Stamping Authority Certificate Policy & Certification Practice Statement:

[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: Requirements for trust service providers issuing EU qualified certificates".

3. Definitions and abbreviations

3.1 Definitions

Term	Definition
ADACOM S.A. or ADACOM	ADACOM S.A. with registered offices in 25, Kreontos Street 10442, Athens Greece
ADACOM Repository	ADACOM’s database of Certificates and other relevant ADACOM information accessible on-line.
Certificate	Public key of a TSA, together with some other information, rendered un-forgeable by encipherment with the private key of the Certification Authority which issued it
Certification Authority (CA)	An entity authorized to create and assign certificates
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
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer
Compliance Audit	A periodic audit that a Processing Center, Service Center or Managed PKI Customer undergoes to determine its conformance with STN Standards that apply to it.

Term	Definition
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.
Coordinated Universal Time (UTC)	Time scale based on the second as defined in ITU-R Recommendation 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.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate 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.
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.
Policy Management Authority (PMA)	The organization within ADACOM responsible for promulgating this policy.
Practice Statement	A statement of the practices that a TSP employs in providing a Trust Service.
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 certificate or to decrypt electronic records or files that were encrypted with the corresponding public key
Processing Center	The ADACOM 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 STN PKI consists of systems that collaborate to provide and implement the STN.
Qualified electronic seal	Is an advanced electronic seal that is created by a qualified electronic seal creation device and is based on a qualified certificate for electronic seals.
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 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 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 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.
Relying Party	An individual or organization that acts in reliance on a certificate or time stamp.
Root CA	Certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s).
Subscriber	An entity which applies for a Time Stamping Service and is legally bound to any Subscriber obligations.

Term	Definition
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.
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 Authority (TSA)	The Authority of the Time Stamping Services, which issues Time Stamp Tokens.
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.
Trust Service	Electronic service for: • creation, verification, and validation of digital signatures and related certificates; • creation, verification, and validation of time-stamps 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.
Trusted Position	The positions within ADACOM that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a “trusted system” as recognized in classified government nomenclature.
TSA Disclosure Statement	Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to Subscribers and Relying Parties,
TSA Practice Statement	Statement of the practices that a TSA employs in issuing Time Stamp Tokens.
TSA System	Composition of IT products and components organized to support the provision of Time Stamping Services.

3.2 Abbreviations

Acronym	Definition
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSU	Cryptographic Signing Unit
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
OID	Object identifier
QTSSP	Qualified Time Stamping Service Provider
RFC	Request for Comments

Acronym	Definition
TSA	Time Stamping Authority
TSP	Time Stamping Policy
TSS	Time Stamping Services
TST	Time Stamp Token
TSSP	Time Stamping Service Provider
TSU	Time Stamping Unit
URL	Uniform Resource Locator
UTC	Coordinated Universal Time

4. General concepts

4.1 Time Stamping Services

ADACOM Qualified Time Stamping Services (QTSS) consists of the management of the infrastructure for, and the provisioning of Time Stamp Tokens. These services are provided by the ADACOM Time Stamping Authority (TSA) to the Subscribers and are an integral part of the ADACOM Public Key Infrastructure (PKI) and in accordance with the eIDAS Regulation and the European Telecommunications Standards Institute standards (ETSI).

ADACOM offers time-stamping services using RFC 3161 Time Stamp Protocol over HTTP transport. Each TST contains Time-Stamping Policy identifier, unique serial number and TSU certificate containing ADACOM TSA identification information

The QTSS assures use of a reliable time source and proper management of all system components.

4.2 Time Stamping Authority

The ADACOM Time Stamping Authority (TSA) is responsible for provisioning of Qualified Time Stamping Services as described in this document. It has the responsibility 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 ADACOM S.A. acting as QTSSP.

ADACOM issues Qualified Time Stamps under the following hierarchy:

Root CA
CN = ADACOM Global Qualified CA
O = ADACOM S.A.
2.5.4.97 = VATEL-099554476
OU = ADACOM Trust Services
C = GR

Time Stamping Authority CA
CN = ADACOM Qualified Timestamping CA
O = ADACOM S.A.
2.5.4.97 = VATEL-099554476
OU = ADACOM Trust Services
C = GR

Time Stamping Unit CA
CN = ADACOM Qualified TSU 2018
O = ADACOM S.A.

2.5.4.97 = VATEL-099554476
OU = ADACOM Trust Services
C = GR

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

- **OID 0.4.0.2042.1.2** itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)
- **OID 0.4.0.2023.1.1**: itu-t(0) identifiedorganization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

4.3 Subscribers

The Subscriber is the applicant, natural or legal person, to whom the time stamp is provided and who enters into the contract with ADACOM.

The Subscriber may be an organization comprising several end-users or an individual end-user.

When the Subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case, the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization shall duly notify its end-users.

When the Subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.3.1 Relying Parties

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

4.3.2 Other Participants

Not applicable.

4.3.3 Time Stamps Usage

Time stamps issued by ADACOM, as specified in this document, are qualified under the eIDAS Regulation. Time Stamps shall be used only to the extent the use is consistent with applicable law and within the limits and contexts specified in the present document. Any use outside of the limits and contexts specified in this document or for unlawful purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of ADACOM is prohibited. Indicatively, 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;
- enabling other parties to use the Subscriber's TST;
- using the Time Stamp issued to time-stamp documents which can bring about unwanted consequences (including time-stamping such documents for testing purposes).

4.4 Time Stamping Policy and TSA Practice Statement

4.4.1 Purpose

The present document specifies policy and security requirements relating to the operation and management practices of the ADACOM as a Time Stamping Authority (TSA) for issuing Qualified Time Stamps. These can be used in support of electronic signatures or for any application requiring to prove that a datum existed before a specific time.

The present document can be used by independent entities as the basis for confirming that ADACOM TSA is a trusted entity of the issuance of Qualified Time Stamps in accordance to eIDAS.

The present document is publicly available. Distribution of this document is restricted as described in the "Intellectual Property Rights" section.

4.4.2 Level of specificity

The present document describes only general rules of issuing and managing TST. Detailed description of the infrastructure and related operational procedures are described in additional documents that are not made publicly available. These additional documents are only available to authorized ADACOM personnel and, on a need-to-know basis, to auditors of the TSS.

4.4.3 Approach

The present document is defined of the specific details of the operating environment, organizational structure, operating procedures, facilities, and computing environment of the ADACOM TSA.

5. Time Stamp Policies

5.1 Overview

The present Policy defines a set of rules used during the issuing of TST and is regulating the security level for the ADACOM TSA. The ADACOM TSA issues TST according to ETSI Standard EN 319 422.

ADACOM TSU issues qualified electronic time-stamps as per eIDAS regulation, ADACOM TSU do not issue non-qualified electronic time-stamps.

TST are issued with an accuracy of one (1) second.

Time-stamps are requested by means of Hypertext Transfer Protocol (HTTP), as described by RFC 3161.

5.2 Identification

The object-identifier (OID) of the ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement is 1.3.6.1.4.1.15976.1.1.3:

1.3.6.1.4.1.15976	Identification Number (OID) of ADACOM, registered to IANA
1.3.6.1.4.1.15976.1	Certification Service Provider
1.3.6.1.4.1.15976.1.1	Qualified Certificate Policies
1.3.6.1.4.1.15976.1.1.3	Qualified Time Stamping Services

This OID is referenced in every ADACOM issued time-stamp token, and the ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement is available to both Subscribers and Relying Parties.

ADACOM issues the TSTs in accordance with ETSI EN 319 421 best practice for time-stamping policy (OID 0.4.0.2023.1.1).

5.3 User Community and Applicability

There are no limitations on users' eligibility or applicability of the services delivered. The ADACOM TSA can provide Time Stamping Services for Time Stamping of any electronic data to any user, including closed communities.

ADACOM does not provide public Time Stamping Services.

5.4 Conformance

The ADACOM TSA uses the identifier in TST as given in section 5.2 "Identification".

The ADACOM TSA ensures compliance of provided services with regulations specified in section 6.1 "TSA Obligations" and ensures reliability of control mechanisms described in section 7 "TSA Practices".

6. Obligations and Liability

6.1 TSA Obligations

6.1.1 General Obligations

This chapter includes, directly or by reference, all the obligations, liabilities, guarantees and responsibilities of the ADACOM TSA, its Subscribers and TST users (Subscribers and Relying Parties). These obligations and responsibilities are regulated by agreements accepted by all parties.

ADACOM operates the ADACOM TSA and assumes responsibility that the requirements of section 7 "TSA Practices" of this document - as well as the provisions of eIDAS, are implemented as applicable to the selected ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement.

ADACOM agreements with Subscribers and Relying Parties describe mutual obligations and responsibilities, including financial responsibilities. The ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement are integral components of these agreements.

6.1.2 TSA Obligations towards Subscribers

ADACOM guarantees an availability of 99.00 % of the ADACOM TSA services in a 24/7 mode excluding scheduled technical breaks, concerning equipment and system conservation.

ADACOM undertakes the following obligations to TSA Subscribers:

- To operate in accordance with this ADACOM Time Stamping Authority 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 maintain a competent and experienced team that can ensure the continuity of the TSS.
- 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 and internal ADACOM policies and procedures.
- To provide high availability access to ADACOM TSA systems except in the case of planned technical interruptions and loss of time synchronization.

6.2 Subscriber Obligations

Subscribers should verify the signatures created by the ADACOM TSA on the TST.

Such verification comprises:

- 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

Subscribers must use secure cryptographic functions for time-stamping requests.

Subscriber obligations are also defined in ADACOM's Terms and Conditions for Use of Qualified Trust Services.

6.3 Relying Party Obligations

Relying parties should verify the signatures created by the ADACOM TSA on the TST.

Such verification comprises:

- 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 ADACOM Time Stamping Authority 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.

Relying parties are expected to use a Trusted List to establish whether the time-stamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified. The qcStatement "esi4-qtstStatement-1" as defined in ETSI EN 319 422 [5], clause 9.1 is used as an indication that the time-stamp is a qualified electronic time-stamp.

6.4 Liability

The liability of ADACOM acting as QTSSP and of Subscribers and Relying Parties connected with the services is specified in the relevant agreement or is as foreseen in the applicable legislation.

ADACOM is responsible for possible damages directly determined, intentionally or by negligence, to any natural or legal person, as a result of failure to comply with the obligations set out in ADACOM Time

Stamping Authority Certificate Policy & Certification Practice Statement and Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014.

ADACOM Terms and Conditions for Use of Qualified Trust Services limit ADACOM's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include a liability cap regarding the combined aggregate liability of ADACOM to any and all persons concerning Time Stamp Services, which is 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 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 shall be the same irrespective to the number of Time Stamps or claims related to such Time Stamp.

ADACOM TSA declines any responsibility with regard to the usage that is made with the TSTs it delivers and signs.

7. TSA Practices

ADACOM TSA shall implement controls that meet ETSI EN 319 421 and ETSI EN 319 422 requirements.

7.1 Practice and Disclosure Statements

7.1.1 TSA Practice Statement

This ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement establishes the general rules concerning the technical, organizational, and procedural requirements of the ADACOM TSA operation.

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.

A risk assessment is regularly carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures that have been taken.

The terms and conditions regarding the use of Time Stamping Services, as included in ADACOM Terms and Conditions for Use of Qualified Trust Services, are disclosed and made available to all Subscribers and Relying Parties as specified in section 7.1.2 of the present document.

ADACOM Policy Management Authority has responsibility for maintaining and approving all ADACOM PKI policies and practices according to the terms of section 1.1 "Policy Administration" of the current document. ADACOM management has responsibility to ensure that the practices are properly implemented.

7.1.2 TSA Disclosure Statement

ADACOM TSA discloses to all Subscribers and potential Relying Parties the terms and conditions regarding use of ADACOM Time Stamping Services.

ADACOM's TSA Disclosure Statement is compliant with requirements of ETSI EN 319 421 and contains statements about the TSA's practice, as well as the rights and obligations of Subscribers and Relying Parties in a simplified and comprehensive way.

Some elements of the ADACOM TSA Disclosure Statement are listed below:

- Every TST issued by ADACOM TSA includes the policy identifier, defined in section 5.2 of the present document.
- Cryptographic hash functions, used in the timestamping process are in accordance with normative requirements, SHA-256 and SHA-512.
- Expected validity period of ADACOM TSU is up to ten (10) years.
- Accuracy of the time, which is provided in a TST, is regulated in section 5.1 of the present document.
- Applicability limitations related with TSA system have been defined in section 5.3 of the present document.
- TST verification should be performed with the usage of appropriate software.
- Subscriber obligations are described in section 6.2 of the present document.
- Relying Party obligations are described in section 6.3 of present document.
- ADACOM maintains secure records concerning the operation of the ADACOM TSA.
- ADACOM may charge fees for the services provided by the ADACOM TSA.

7.2 Key Management Life Cycle

7.2.1 TSA Key Generation

Personnel in trusted roles under dual control perform the generation of the TSU signing keys in a physically secured environment. The personnel authorized to carry out this function are limited to those required to do so under the TSA practices.

The generation of the TSU signing keys is carried out within secure cryptographic devices, which meets the requirements identified in FIPS 140-2 level 3.

Key Pairs are generated using secure algorithms and parameters based on current research and industry standards following the recommendations of ETSI TS 319 312.

The activities performed in each key generation are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by ADACOM Management.

7.2.2 TSU Private Key Protection

ADACOM takes specific steps to ensure that TSU private keys remain confidential and maintain their integrity.

TSU private keys are stored in a secure Hardware Security Module to perform key signing operations, which comply with at least FIPS 140-2 level 3 or equivalent EAL 4+ or higher in accordance to ISO/IEC 15408 specifications. Special controls are in place to ensure that the hardware has not been tampered and is functioning correctly.

TSU private keys cannot be extracted in any form and are not accessible outside the Hardware Security Module.

ADACOM creates backup copies of TSU private keys, for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules. Cryptographic modules used for private key storage meet the requirements of this CPS. Private keys are copied to backup hardware cryptographic modules. Restoring of TSU backup keys require dual control in a physically secured environment.

7.2.3 TSU Public Key Distribution

ADACOM TSU Public Keys are made available in a Digital Certificate.

ADACOM TSU Certificates are available for secure download via the ADACOM Repository website https://pki.adacom.com/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).

7.2.4 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.

ADACOM TST are signed with ADACOM TSU certificates of ten (10) years validity. ADACOM TSU certificates of ten (10) years validity are only used to sign TST during a usage period of one (1) year.

ADACOM 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.

7.2.5 End of TSU Key Life Cycle

ADACOM 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.

7.2.6 Life Cycle Management of the Cryptographic Module used to Sign Time-stamps

ADACOM TSA ensures the security of the HSM throughout its lifecycle.

ADACOM 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 according with the manufacturer's instructions.

7.3 Time-stamping

7.3.1 Time-stamp Token

ADACOM 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 to identify specific TST
- a unique identifier of the policy as described in section 5.2 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

ADACOM TSUs maintain audit logs for all calibrations against the UTC references.

7.3.2 Clock Synchronization with UTC

The ADACOM TSA ensures that its time is synchronised with UTC within the declared accuracy with multiple independent time sources. ADACOM TSA incorporates the time in the TST with the accuracy described in section 5.1 of the present document.

Audit and calibration records of the synchronization are maintained by ADACOM. ADACOM 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.

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

7.3.3 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.

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

7.4 TSA Management and Operation

7.4.1 Security Management

ADACOM TSA ensures that administrative and management procedures are applied which are adequate and correspond to recognized best practices.

ADACOM performs all TSA functions using trustworthy systems that meet the requirements of ADACOM ISMS.

7.4.2 Asset Classification and Management

ADACOM maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

7.4.3 Personnel Security

ADACOM maintains appropriate personnel controls fulfilling security best practice and the requirements of relevant standards.

Managerial and operational personnel possess the appropriate skills and knowledge of Time Stamping, digital signatures and Trust Services as well as security procedures for personnel with security responsibilities, information security and risk assessment.

Trusted Persons include all employees that have access to or control cryptographic operations. Trusted Persons include, but are not limited to:

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

For all personnel seeking to become Trusted Persons, verification of identity is performed through the ADACOM HR process based on check of well-recognized forms of identification (e.g., passports or identification cards). Identity is further confirmed through the background checking procedures.

ADACOM ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities;
- Issued electronic credentials to access and perform specific functions on ADACOM CA, TSA, or other IT systems.

ADACOM has implemented an access control system, which identifies authorities and registers all the ADACOM information system users in a trustworthy manner.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with dedicated account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are locked as soon as possible when the role change dictates. Access rules are audited annually.

ADACOM requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities, as specified in the employment contract, job description and Roles and Responsibilities documents, competently and satisfactorily as well as proof of any government clearances, if any, necessary to perform certification services under government contracts, before they perform any operational or security functions.

The employment contracts signed by the employees of ADACOM provide for the following obligations:

- To maintain the secrecy of confidential information that has come to their knowledge in the course of their performance,
- To prevent them from holding business interests in a company, which may affect their judgment in the supply of the service
- To ensure that they have not been punished for a willful crime.
- All personnel in Trusted Roles are free from any interests that may affect their impartiality regarding ADACOM operations.

Prior to commencement of employment in a Trusted Role, ADACOM conducts background checks which include the following:

- Verification of identity
- Check of previous employment and professional reference (if available);
- Confirmation of the highest or most relevant educational degree obtained;
- Search of national criminal records;
- Check of financial records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, ADACOM will utilize a substitute investigative technique permitted by law that provides substantially similar information.

7.4.4 Physical and Environmental Security

ADACOM has implemented the ADACOM Physical Security Policy, which supports the security requirements of this CP/CPS. Compliance with these policies is included in ADACOM's audit requirements. ADACOM Physical Security Policy contains sensitive security information and is only available upon agreement with ADACOM.

ADACOM CA and TSA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

ADACOM also maintains Disaster Recovery facilities for its Time Stamping Services operations. ADACOM's Disaster Recovery facilities are protected by multiple tiers of physical security comparable to those of ADACOM's primary facility.

ADACOM systems are protected by seven (7) tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive TSA operational activity and any activity related to the lifecycle of the certification process, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Some tiers enforce individual access control through the concurrent use of proximity cards and biometrics (two factor authentication). Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes tiers for key management security which serves to protect both online and offline storage of Cryptographic Signing Unit (CSUs) and keying material. Areas used to create and store cryptographic material enforce dual control, each through the concurrent use of proximity cards and biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with ADACOM's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

ADACOM operations are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of buildings requires the use of an "access" or "pass" card. Access card use is logged by the building security system.

Access card logs and video records are reviewed on a regular basis. ADACOM securely stores all removable media and paper containing sensitive plain-text information related to its operations in secure containers.

ADACOM's secure facilities 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.

ADACOM has taken reasonable precautions to minimize the impact of water exposure to ADACOM systems

ADACOM has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. ADACOM's fire prevention and protection measures have been designed to comply with local fire safety regulations.

All media containing production software and data, audit, archive, or backup information is stored within ADACOM facilities or in a secure off-site storage facility with appropriate physical and logical access

controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire).

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. Other waste is disposed of in accordance with ADACOM's normal waste disposal requirements.

7.4.5 Operations Management

ADACOM TSA ensures that the procedures, processes and infrastructure to comply with the operational management, procedural security requirements, system access management, trustworthy systems deployment and maintenance, business continuity management and incident handling as defined in ETSI EN 319 421.

The operations management procedures for the ADACOM TSA are incorporated within the overall ADACOM internal operations management procedures.

7.4.6 Trustworthy Systems Deployment and Maintenance

ADACOM ensures that the systems maintaining TSA software and data files are trustworthy systems secure from unauthorized access and modification. In addition, ADACOM limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

7.4.7 Compromise of TSA Services

In the case of compromise to a TSU's 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 the ADACOM makes available to all Subscribers and Relying Parties a description of compromise that occurred.
In case of major compromise of the TSA's operation, ADACOM 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 TSAs users or the security of the TSA services.

7.4.8 TSA Termination

The TSA is terminated:

- with a decision of ADACOM's Board of Directors or Managing Director;
- 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 ADACOM.

ADACOM ensures that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of ADACOM's 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 an ADACOM TSA, to cease operation, ADACOM makes a commercially reasonable effort to notify Subscribers and Relying Parties of such termination in advance of the TSA termination.

ADACOM TSA revokes the TSU's certificates when it terminates its services.

7.4.9 Compliance with Legal Requirements

ADACOM 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 23 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

ADACOM acting as QTSP accepts compliance audit for its TSA and Time Stamping Services to ensure they meet the eIDAS requirements.

7.4.10 Recording of Information Concerning Operation of Time Stamping Services

ADACOM TSA ensures that all relevant information concerning the operations of the ADACOM Time Stamping Services is recorded for a defined period, in particular for providing evidence for the purposes of legal proceedings.

ADACOM maintains records of all relevant information concerning the operation of the ADACOM TSA for the time period specified in Section 7.1.1.

The ADACOM 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.

7.4.11 Organizational

ADACOM TSA ensures that its organization is reliable as required in ETSI EN 319 421. ADACOM has the financial stability and resources required to operate in conformity with current ADACOM Time Stamping Authority Certificate Policy & Certification Practice Statement.

Important policy and practice documents for the ADACOM TSA are available at https://pki.adacom.com/repository.