



**ADACOM S.A.  
Certification Practice Statement  
for EU Qualified certificates for  
electronic signatures and  
electronic seals**

**Version 3.4**

**Effective Date: 25/01/2019**

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

## **ADACOM Certification Practices Statement for EU Qualified certificates for electronic signatures and electronic seals**

© 2019 ADACOM SA. All rights reserved.

### **Trademark Notices**

ADACOM is the registered mark of ADACOM SA. Symantec, the Symantec logo, and the Checkmark Logo are the registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. The VeriSign logo, VeriSign Trust and other related marks are the trademarks or registered marks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed by Symantec Corporation. Other names may be trademarks of their respective owners.

Without limiting the rights reserved above, and 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.

Notwithstanding the above, permission is granted to reproduce and distribute this ADACOM Certification Practice Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to ADACOM S.A.

Requests for any other permission to reproduce this ADACOM Certification Practices Statement (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, Net: [practices@adacom.com](mailto:practices@adacom.com).

Version History		
Date	Version	Changes
24.02.2017	1.0	Initial document
10.04.2017	2.0	Minor changes regarding chapter 1.3
27.04.2017	2.1	Contact info update
18.05.2018	3.0	Minor changes and addition of remote QSCD services.
29.06.2018	3.1	Minor changes regarding paragraphs 1.4.2, 3.1.5, 3.2, 4.9.2, 4.9.7, 5.7.3, 6.1.2 & 6.2.1
01.11.2018	3.2	Minor changes in paragraphs 4.2.3, 4.3.1 and 4.9.2.
10.01.2019	3.3	Minor changes in paragraphs 4.9.2 and 4.9.3
25.01.2019	3.4	Minor changes in paragraphs 4.9.1, 4.9.3 and 6.6.3, addition of Remote ID verification as authentication method in par.3.2.3, addition of Short-lived/Long-lived Certificate Definition

## **Table of Contents**

1. INTRODUCTION.....	9
1.1 Overview.....	9
1.2 Document name and Identification.....	11
1.3 PKI Participants.....	11
1.3.1 Certification Authorities.....	11
1.3.2 Registration Authorities.....	12
1.3.3 Local Registration Authorities.....	12
1.3.4 Subscribers.....	13
1.3.5 Relying Parties.....	13
1.3.6 Other Participants.....	13
1.4 Certificate Usage.....	13
1.4.1 Appropriate Certificate Usages.....	13
1.4.2 Prohibited Certificate Uses.....	14
1.5 Policy Administration.....	14
1.5.1 Organization Administering the Document.....	14
1.5.2 Contact Person.....	14
1.5.3 Person Determining CP Suitability for the Policy.....	14
1.5.4 CPS Approval Procedure.....	14
1.6 Definitions and Acronyms.....	15
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	15
2.1 Repositories.....	15
2.2 Publication of Certificate Information.....	15
2.2.1 Publication and Notification Policies.....	15
2.2.2 Items not published in the Certification Practice Statement.....	16
2.3 Time or Frequency of Publication.....	16
2.4 Access Controls on Repositories.....	16
3. IDENTIFICATION AND AUTHENTICATION.....	16
3.1 Naming.....	16
3.1.1 Type of Names.....	16
3.1.2 Need for Names to be Meaningful.....	16
3.1.3 Anonymity or Pseudonymity of Subscribers.....	16
3.1.4 Rules for Interpreting Various Name Forms.....	16
3.1.5 Uniqueness of Names.....	17
3.1.6 Recognition, Authentication, and Role of Trademarks.....	17
3.2 Initial Identity Validation.....	17
3.2.1 Method to Prove Possession of Private Key.....	17
3.2.2 Authentication of Organization identity.....	17
3.2.3 Authentication of Individual Identity.....	18
3.2.4 Non-Verified Subscriber information.....	19
3.2.5 Validation of Authority.....	19
3.3 Identification and Authentication for Re-key Requests.....	19
3.3.1 Identification and Authentication for Routine Re-key.....	19
3.3.2 Identification and Authentication for Re-key After Revocation.....	19
3.4 Identification and Authentication for Revocation Request.....	20

4.	CERTIFICATE LIFE-CYCLE OPERATIONAL.....	20
4.1	Certificate Application.....	20
4.1.1	Who Can Submit a Certificate Application?.....	20
4.1.2	Enrollment Process and Responsibilities.....	20
4.2	Certificate Application Processing.....	20
4.2.1	Performing Identification and Authentication Functions.....	20
4.2.2	Approval or Rejection of Certificate Applications.....	21
4.2.3	Time to Process Certificate Applications.....	21
4.3	Certificate Issuance.....	21
4.3.1	CA Actions during Certificate Issuance.....	21
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate.....	21
4.4	Certificate Acceptance.....	21
4.4.1	Conduct Constituting Certificate Acceptance.....	21
4.4.2	Publication of the Certificate by the CA.....	22
4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	22
4.5	Key Pair and Certificate Usage.....	22
4.5.1	Subscriber Private Key and Certificate Usage.....	22
4.5.2	Relying Party Public Key and Certificate Usage.....	22
4.6	Certificate Renewal.....	23
4.7	Certificate Re-Key.....	23
4.7.1	Circumstances for Certificate Re-Key.....	23
4.7.2	Who May Request Certification of a New Public Key.....	23
4.7.3	Processing Certificate Re-Keying Requests.....	23
4.7.4	Notification of New Certificate Issuance to Subscriber.....	23
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate.....	23
4.7.6	Publication of the Re-Keyed Certificate by the CA.....	23
4.7.7	Notification of Certificate Issuance by the CA to Other Entities.....	23
4.8	Certificate Modification.....	24
4.8.1	Circumstances for Certificate Modification.....	24
4.8.2	Who May Request Certificate Modification.....	24
4.8.3	Processing Certificate Modification Requests.....	24
4.8.4	Notification of New Certificate Issuance to Subscriber.....	24
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	24
4.8.6	Publication of the Modified Certificate by the CA.....	24
4.8.7	Notification of Certificate Issuance by the CA to Other Entities.....	24
4.9	Certificate Revocation and Suspension.....	24
4.9.1	Circumstances for Revocation.....	24
4.9.2	Who Can Request Revocation.....	25
4.9.3	Procedure for Revocation Request.....	25
4.9.4	Revocation Request Grace Period.....	26
4.9.5	Time within Which CA Must Process the Revocation Request.....	26
4.9.6	Revocation Checking Requirements for Relying Parties.....	26
4.9.7	CRL Issuance Frequency.....	26
4.9.8	Maximum Latency for CRLs.....	26
4.9.9	On-Line Revocation/Status Checking Availability.....	26
4.9.10	On-Line Revocation Checking Requirements.....	27

4.9.11	Other Forms of Revocation Advertisements Available.....	27
4.9.12	Special Requirements regarding Key Compromise.....	27
4.9.13	Circumstances for Suspension.....	27
4.9.14	Who Can Request Suspension.....	27
4.9.15	Procedure for Suspension Request.....	27
4.9.16	Limits on Suspension Period.....	27
4.10	Certificate Status Services.....	27
4.10.1	Operational Characteristics.....	27
4.10.2	Service Availability.....	27
4.10.3	Optional Features.....	28
4.11	End of Subscription.....	28
4.12	Key Escrow and Recovery.....	28
4.12.1	Key Escrow and Recovery Policy and Practices.....	28
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	28
5.	<b>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.</b>	28
5.1	Physical Controls.....	28
5.1.1	Site Location and Construction.....	28
5.1.2	Physical Access.....	28
5.1.3	Power and Air Conditioning.....	29
5.1.4	Water Exposures.....	29
5.1.5	Fire Prevention and Protection.....	29
5.1.6	Media Storage.....	29
5.1.7	Waste Disposal.....	29
5.1.8	Off-Site Backup.....	30
5.2	Procedural Controls.....	30
5.2.1	Trusted Roles.....	30
5.2.2	Number of Persons Required per Task.....	30
5.2.3	Identification and Authentication for Each Role.....	31
5.2.4	Roles Requiring Separation of Duties.....	31
5.3	Personnel Controls.....	31
5.3.1	Qualifications, Experience, and Clearance Requirements.....	31
5.3.2	Background Check Procedures.....	32
5.3.3	Training Requirements.....	32
5.3.4	Retraining Frequency and Requirements.....	33
5.3.5	Job Rotation Frequency and Sequence.....	33
5.3.6	Sanctions for Unauthorized Actions.....	33
5.3.7	Independent Contractor Requirements.....	33
5.3.8	Documentation Supplied to Personnel.....	33
5.4	Audit Logging Procedures.....	33
5.4.1	Types of Events Recorded.....	33
5.4.2	Frequency of Processing Log.....	34
5.4.3	Retention Period for Audit Log.....	34
5.4.4	Protection of Audit Log.....	35
5.4.5	Audit Log Backup Procedures.....	35
5.4.6	Audit Collection System (Internal vs. External).....	35
5.4.7	Notification to Event-Causing Subject.....	35

5.4.8	Vulnerability Assessments.....	35
5.5	Records Archival.....	35
5.5.1	Types of Records Archived.....	35
5.5.2	Retention Period for Archive.....	35
5.5.3	Protection of Archive.....	35
5.5.4	Archive Backup Procedures.....	36
5.5.5	Requirements for Time-Stamping of Records.....	36
5.5.6	Archive Collection System (Internal or External).....	36
5.5.7	Procedures to Obtain and Verify Archive Information.....	36
5.6	Key Changeover.....	36
5.7	Compromise and Disaster Recovery.....	37
5.7.1	Incident and Compromise Handling Procedures.....	37
5.7.2	Computing Resources, Software, and/or Data Are Corrupted.....	37
5.7.3	Entity Private Key Compromise Procedures.....	37
5.7.4	Business Continuity Capabilities after a Disaster.....	37
5.8	CA or RA Termination.....	38
6.	<b>TECHNICAL SECURITY CONTROLS.....</b>	<b>39</b>
6.1	Key Pair Generation and Installation.....	39
6.1.1	Key Pair Generation.....	39
6.1.2	Private Key Delivery to Subscriber.....	39
6.1.3	Public Key Delivery to Certificate Issuer.....	39
6.1.4	CA Public Key Delivery to Relying Parties.....	40
6.1.5	Key Sizes.....	40
6.1.6	Public Key Parameters Generation and Quality Checking.....	40
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field).....	40
6.2	Private Key Protection and Cryptographic Module Engineering Controls.....	40
6.2.1	Cryptographic Module Standards and Controls.....	40
6.2.2	Private Key (m out of n) Multi-Person Control.....	41
6.2.3	Private Key Escrow.....	41
6.2.4	Private Key Backup.....	41
6.2.5	Private Key Archival.....	41
6.2.6	Private Key Transfer Into or From a Cryptographic Module.....	41
6.2.7	Private Key Storage on Cryptographic Module.....	42
6.2.8	Method of Activating Private Key.....	42
6.2.9	Method of Deactivating Private Key.....	42
6.2.10	Method of Destroying Private Key.....	43
6.2.11	Cryptographic Module Rating.....	43
6.3	Other Aspects of Key Pair Management.....	43
6.3.1	Public Key Archival.....	43
6.3.2	Certificate Operational Periods and Key Pair Usage Periods.....	43
6.4	Activation Data.....	44
6.4.1	Activation Data Generation and Installation.....	44
6.4.2	Activation Data Protection.....	44
6.4.3	Other Aspects of Activation Data.....	44
6.5	Computer Security Controls.....	44
6.5.1	Specific Computer Security Technical Requirements.....	44

6.5.2	Computer Security Rating.....	45
6.6	Life Cycle Technical Controls.....	45
6.6.1	System Development Controls.....	45
6.6.2	Security Management Controls.....	46
6.6.3	Life Cycle Security Controls.....	46
6.7	Network Security Controls.....	46
6.8	Time-Stamping.....	46
7.	CERTIFICATE, CRL, AND OCSP PROFILES.....	46
7.1	Certificate Profile.....	46
7.2	CRL Profile.....	47
7.3	OCSP Profile.....	47
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	47
8.1	Frequency and Circumstances of Assessment.....	47
8.2	Identity/Qualifications of Assessor.....	47
8.3	Assessor's Relationship to Assessed Entity.....	47
8.4	Topics Covered by Assessment.....	47
8.5	Actions Taken as a Result of Deficiency.....	48
8.6	Communications of Results.....	48
9.	OTHER BUSINESS AND LEGAL MATTERS.....	49
9.1	Fees.....	49
9.1.1	Certificate Issuance or Renewal Fees.....	49
9.1.2	Certificate Access Fees.....	49
9.1.3	Revocation or Status Information Access Fees.....	49
9.1.4	Fees for Other Services.....	49
9.1.5	Refund Policy.....	49
9.2	Financial Responsibility.....	50
9.2.1	Insurance Coverage.....	50
9.2.2	Other Assets.....	50
9.2.3	Insurance or Warranty Coverage for End-Entities.....	50
9.3	Confidentiality of Business Information.....	50
9.3.1	Scope of Confidential Information.....	50
9.3.2	Information Not Within the Scope of Confidential Information.....	50
9.3.3	Responsibility to Protect Confidential Information.....	50
9.4	Privacy of Personal Information.....	50
9.4.1	Privacy Plan.....	50
9.4.2	Information Treated as Private.....	51
9.4.3	Information Not Deemed Private.....	51
9.4.4	Responsibility to Protect Private Information.....	51
9.4.5	Notice and Consent to Use Private Information.....	51
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	51
9.4.7	Disclosure upon Owner's Request.....	51
9.4.8	Other Information Disclosure Circumstances.....	51
9.5	Intellectual Property rights.....	51
9.5.1	Property Rights in Certificates and Revocation Information.....	51
9.5.2	Property Rights in the CPS.....	52
9.5.3	Property Rights in Names.....	52

9.5.4	Property Rights in Keys and Key Material.....	52
9.6	Representations and Warranties.....	52
9.6.1	CA Representations and Warranties.....	52
9.6.2	RA Representations and Warranties.....	53
9.6.3	Subscriber Representations and Warranties.....	53
9.6.4	Relying Party Representations and Warranties.....	54
9.6.5	Representations and Warranties of Other Participants.....	54
9.7	Disclaimers of Warranties.....	54
9.8	Limitations of Liability.....	54
9.9	Indemnities.....	55
9.9.1	Indemnification by Subscribers.....	55
9.9.2	Indemnification by Relying Parties.....	55
9.10	Term and Termination.....	55
9.10.1	Term.....	55
9.10.2	Termination.....	55
9.10.3	Effect of Termination and Survival.....	55
9.11	Individual Notices and Communications with Participants.....	56
9.12	Amendments.....	56
9.12.1	Procedure for Amendment.....	56
9.12.2	Notification Mechanism and Period.....	56
9.12.3	Circumstances under Which OID Must be changed.....	56
9.13	Dispute Resolution Provisions.....	57
9.13.1	Disputes among Symantec, Affiliates, and Customers.....	57
9.13.2	Disputes with Subscribers or Relying Parties.....	57
9.14	Governing Law.....	57
9.15	Compliance with Applicable Law.....	57
9.16	Miscellaneous Provisions.....	57
9.16.1	Entire Agreement.....	57
9.16.2	Assignment.....	58
9.16.3	Severability.....	58
9.16.4	Enforcement (Attorney's Fees and Waiver of Rights).....	58
9.16.5	Force Majeure.....	58
9.17	Other Provisions.....	58
Appendix A. Table of Acronyms and definitions.....		59
Table of Acronyms.....		59
Definitions.....		59



# 1. INTRODUCTION

This document is the ADACOM Certification Practice Statement (“CPS”) for EU Qualified Certificates. It states the practices that ADACOM Trusted Service Provider (TSP) employs in providing certification services for EU Qualified Certificates for electronic signatures and EU Qualified Certificates for electronic seals in accordance but not limited to Articles 19, 24, 28, 38 and 45 of Regulation (EU) N° 910/2014 [eIDAS] and with the specific requirements of the Symantec Trust Network Certificate Policies (“CP”)

The CP is the principal statement of policy governing the Symantec Trust Network (STN). It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STN and providing associated trust services. These requirements, called the “STN Standards,” protect the security and integrity of the STN, apply to all STN Participants, and thereby provide assurances of uniform trust throughout the STN. More information concerning the STN and STN Standards is available in the CP.<sup>1</sup>

ADACOM has authority over a portion of the STN called its “Sub-domain” of the STN. ADACOM's Sub-domain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CP set forth requirements that STN Participants must meet, this CPS describes how ADACOM meets these requirements in accordance with Regulation (EU) N° 910/2014 and within ADACOM's Sub-domain of the STN. More specifically, this CPS describes the practices that ADACOM employs for:

- Securely managing the related infrastructure that supports the STN, and
- Issuing, maintenance and life-cycle management of EU Qualified Certificates as defined in Regulation (EU) N° 910/2014

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

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

## 1.1 Overview

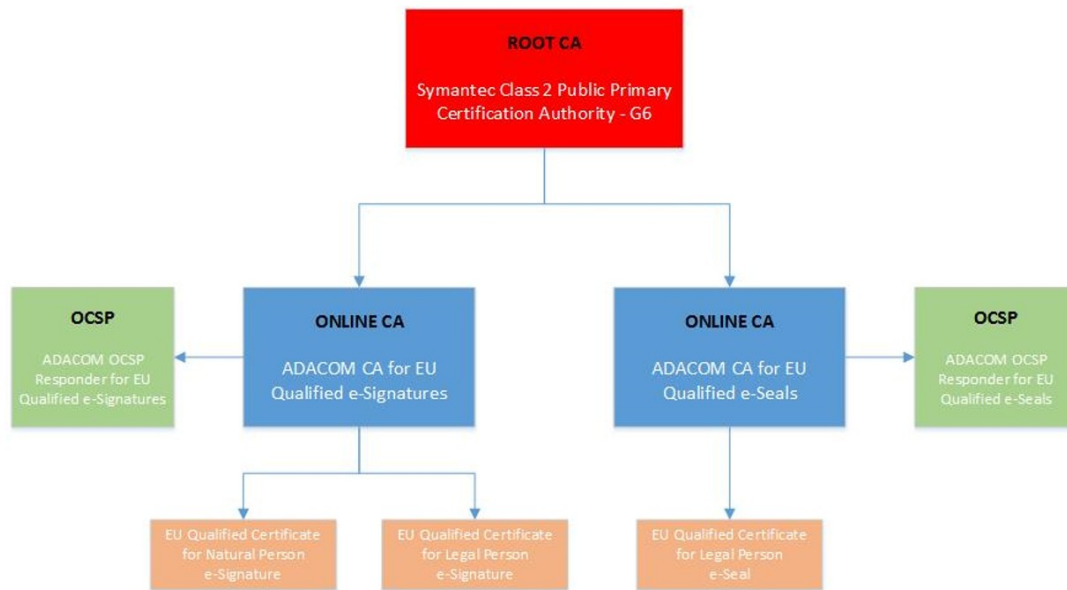
This CPS describes the practices and procedures used to address all the requirements identified by Regulation (EU) N° 910/2014, for issuing, maintenance and lifecycle management of EU Qualified Certificates for electronic signatures and EU Qualified Certificates for electronic seals.

These practices and procedures are compliant with ETSI EN 319 411-2 Policy: QCP-n-qscd for EU Qualified Certificates for electronic signatures and Policy: QCP-l-qscd for EU Qualified Certificates for electronic seals and with ETSI EN 319 411-1 Policy: extended Normalized Certificate Policy (NCP+)

ADACOM is currently using the following certificate chain:

---

<sup>1</sup> The current version of STN CP, can be found at <https://pki.adacom.com/repository>



ADACOM has established a secure facility housing, among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of Certificates. ADACOM acts as a CA in the STN and performs all Certificate lifecycle services of issuing, managing, revoking, and renewing EU Qualified Certificates.

This CPS is specifically applicable to:

- ADACOM's Issuing CAs, who issue EU Qualified Certificates for electronic signatures and electronic seals

Private CAs and other hierarchies that are managed by ADACOM but are not mentioned in this document are outside the scope of this CPS. The practices relating to services provided by other Organizations or services provided by ADACOM to other Organizations are beyond the scope of this CPS. The CAs managed by other Organizations are also outside the scope of this CPS.

ADACOM publishes the Certificate Practices Statement in order to comply with the specific policy requirements of the applicable legislation, or other industry standards and requirements.

The CPS is only one of a set of documents relevant to ADACOM's Trust Services. These other documents include:

- Ancillary confidential security and operational documents<sup>3</sup> that supplement the CPS by providing more detailed requirements, such as:
  - Key Ceremony Reference Guide, which presents detailed key management operational requirements.
  - The ADACOM Physical Security Policy which sets forth security principles governing ADACOM infrastructure,
  - The ADACOM Information System Security Policy that states the requirements for Information System infrastructure in order to operate securely and according to relative legislative and contractual requirements.
  - ADACOM Cryptographic Key Management Policy, which presents detailed key management operational requirements.

3

<sup>3</sup> Although these documents are not publicly available their specifications are included in ADACOM's Conformity Assessment Report for Trust Service Providers issuing EU Qualified certificates and may be made available to customer under special agreement,

- General Terms and Conditions imposed by ADACOM. These General Terms and Conditions bind Customers, Subscribers and Relying Parties of ADACOM. Among other things, the General Terms and conditions cover a broad range of commercial terms or ADACOM Trust Services specific terms.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing ADACOM and STN Policies where including the specifics in the CPS could compromise the security of ADACOM's Sub-domain of the STN.

## **1.2 Document name and Identification**

This document is the ADACOM Certification Practice Statement for EU Qualified Certificates and contain object identifier values corresponding to the applicable STN Class of Certificate according to Symantec CP § 1.2. Therefore, ADACOM has not assigned this CPS an object identifier value.

Certificate Policy Object Identifiers, are used in accordance with Section 7.1

## **1.3 PKI Participants**

### **1.3.1 Certification Authorities**

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates, is called the CA. The CA has overall responsibility for the provision of the certification services. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA). PCAs act as roots. Each PCA is a Symantec entity. Subordinate to the PCAs are ADACOM Certification Authorities that issue EU Qualified Certificates to Subscribers.

ADACOM operates as a Certification Authority that issues EU Qualified Certificates under the following CA hierarchy:

#### **Root CA**

*CN = Symantec Class 2 Public Primary Certification Authority - G6*  
*OU = Symantec Trust Network*  
*O = Symantec Corporation*  
*C = US*

#### **Issuing CAs**

*CN = ADACOM CA for EU Qualified e-Signatures*  
*2.5.4.97 = VATEL-099554476*  
*OU = Adacom Trust Services*  
*OU = Class 2 Managed PKI Individual Subscriber CA*  
*OU = Symantec Trust Network*  
*O = ADACOM S.A.*  
*C = EL*

*CN = ADACOM CA for EU Qualified e-Seals*  
*2.5.4.97 = VATEL-099554476*  
*OU = Adacom Trust Services*  
*OU = Class 2 Managed PKI Individual Subscriber CA*  
*OU = Symantec Trust Network*

O = ADACOM S.A.

C = EL

Adacom CA Certificates are issued according to the following certificate policies:

- **OID 2.16.840.1.113733.1.7.23.2** joint-iso-itu-t(2) country(16) us(840) organization(1) symantec(113733) pki(1) policies(7) vtn-cp(23) class2(2);
- **OID 0.4.0.194112.1.2** itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
- **OID 0.4.0.194112.1.3** itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)
- **OID 0.4.0.2042.1.2** itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)

### 1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and validation of Subscribers for issuing Certificates, initiates or passes along revocation requests for Certificates, and approves applications for re-keying certificates on behalf of the CA. ADACOM acts as an RA for the EU Qualified Certificates it issues.

ADACOM has the authority to enter into a contractual relationship with one or more third parties, in order to outsource part of RA responsibilities, especially regarding the validation of the Subscriber. In this case, the third party constitutes a Local Registration Authority (LRA). LRA performs its responsibilities in full compliance with this CPS, the respective Validation plans and the terms of the LRA Agreement signed between LRA and ADACOM.

ADACOM trains LRA's authorized employees on validation process and security procedures, prior starting LRA's related operations. Thereafter, ADACOM re-trains yearly LRA's authorized employees.

ADACOM performs yearly audits to the LRA operations and procedures in order to ensure compliance with this CPS, the Validation Plans and the LRA Agreement.

### 1.3.3 Local Registration Authorities

A Local Registration Authority is 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. The relationship between LRA and RA is described in the LRA's contract agreement and includes, but not limited, the following:

- Full details of LRA's authorized employees, that will perform LRA's duties and activities;
- LRA's obligation to receive yearly training of LRA's authorized employees from ADACOM regarding LRA's duties and activities and to accept yearly audits by ADACOM regarding LRA operations and procedures;
- LRA's authorized employees obligation to use credentials issued by ADACOM RA to ensure secure communications between both parties;
- LRA's obligation to process Subscribers' applications exclusively through LRA's authorized employees

Local Registration Authority is responsible for delivering the Qualified Signature Creation Device (QSCD) or authentication credentials in case of Remote Qualified Certificate to the Subscriber or Subject.

Local Registration Authority passes all Subscriber's applications or requests accompanied by the related documents to the Registration Authority for approval or rejection of Certificate issuance, re-keying or revocation.

### **1.3.4 Subscribers**

Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with ADACOM for the issuance of credentials and; "Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

Subscriber means a natural or legal person to whom ADACOM provides the Trust Services according to this CPS.

The subject means:

- a natural person
- a natural person who is identified in association with a legal person
- a legal person

The Subscriber may or may not be the Subject of a certificate. The link between the subscriber and the subject is one of the following:

- To request a certificate for natural person the subscriber is:
  - a) the natural person itself;
  - b) a natural person mandated to represent the subject; or
  - c) any entity with which the natural person is associated.
- To request a certificate for legal person the subscriber is:
  - a) any entity as allowed under the relevant legal system to represent the legal person; or
  - b) a legal representative of a legal person subscribing for its subsidiaries or units or departments.

### **1.3.5 Relying Parties**

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the CA. A Relying party may, or may not also be a Subscriber.

### **1.3.6 Other Participants**

Not applicable.

## **1.4 Certificate Usage**

### **1.4.1 Appropriate Certificate Usages**

#### **1.4.1.1 Certificates Issued for electronic signature**

Certificates are compliant with NCP+ and QCP-n-qscd.

Certificates issued under these requirements are aimed to support qualified electronic signatures with the use of a Qualified Signature Creation Device (QSCD) such as defined in article 3 (12) of the Regulation (EU) N° 910/2014 [i.1].

#### **1.4.1.2 Certificates Issued for electronic seals**

Certificates are compliant with NCP+ and QCP-lqscd.

Certificates issued under these requirements are aimed to support qualified electronic seals with the use of a Qualified Signature Creation Device (QSCD) such as defined in article 3 (27) of the Regulation (EU) N° 910/2014 [i.1].

### **1.4.2 Prohibited Certificate Uses**

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

CA Certificates may not be used for any functions except CA functions. In addition, Subscriber Certificates shall not be used as CA Certificates. Usage of Certificates, other than to support applications identified in Section 1.4.1 of the present CPS or in the applicable CP, is prohibited.

Symantec and ADACOM periodically rekey Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. ADACOM therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. ADACOM recommends the use of PCA Roots as root certificates.

## **1.5 Policy Administration**

### **1.5.1 Organization Administering the Document**

ADACOM S.A.  
25, Kreontos Street  
10442, Athens  
Greece

### **1.5.2 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

### **1.5.3 Person Determining CP Suitability for the Policy**

The ADACOM Policy Management Authority (PMA) determines the suitability and applicability of this CPS.

### **1.5.4 CPS Approval Procedure**

Approval of this 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 CPS. The PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies.

## **1.6 Definitions and Acronyms**

See Appendix A for a table of acronyms and definitions.

# **2. PUBLICATION AND REPOSITORY RESPONSIBILITIES**

## **2.1 Repositories**

ADACOM is responsible for the repository functions for its own CAs. ADACOM publishes the issued Certificates in the repository in accordance with section 2.2.

Upon revocation of a Subscriber's Certificate, ADACOM publishes notice of such revocation in the repository. ADACOM issues Certificate Revocation Lists (CRLs) and provides OCSP services pursuant to the provisions of this CPS.

ADACOM shall ensure that its repository is available 24 hours a day, 7 days a week, with a minimum of 99,00% availability overall per year with a scheduled down-time that does not exceed 0,3% annually.

Upon system failure, service or other factors which are not under the control of ADACOM, ADACOM shall apply best endeavours to ensure that this information service is not unavailable for longer than above time.

## **2.2 Publication of Certificate Information**

ADACOM maintains a web-based repository in a public data communications network (<https://pki.adacom.com/repository>) that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. ADACOM provides Relying Parties with information on how to find the appropriate repository to check Certificate status and how to find the right OCSP responder.

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

- Overview of the certification hierarchy
- Certification Practice Statement
- Audit results
- Insurance Policies
- Certification Policies
- Certificates, including root and issuing CAs
- Profiles
- General Terms and Conditions for use of EU Qualified Certificates
- Certificate Revocation Lists
- Certificate search
- Privacy Policies

### **2.2.1 Publication and Notification Policies**

This ADACOM CPS is published in ADACOM's public information repository.

ADACOM CPS along with the enforcement dates is published no less than 30 days prior taking effect.

### **2.2.2 Items not published in the Certification Practice Statement**

Refer to Section 9.3.1 of this CPS.

### **2.3 Time or Frequency of Publication**

Refer to section 2.2.1 of current CPS for updates to this CPS. Updates to Subscriber and Relying Party General Terms and Conditions are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with the provisions of this CPS.

### **2.4 Access Controls on Repositories**

Information published in the repository portion of the ADACOM web site is publicly-accessible information. Read only access to such information is unrestricted. ADACOM requires persons to agree to General Terms and Conditions as a condition to accessing Certificates, Certificate status information, or CRLs. ADACOM has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries according to the applicable ADACOM security policies. ADACOM makes its repository publicly available in a read only manner, and specifically at the link <https://pki.adacom.com/repository>.

## **3. IDENTIFICATION AND AUTHENTICATION**

### **3.1 Naming**

Naming in certificates are as specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7] and the appropriate part of ETSI EN 319 412

#### **3.1.1 Type of Names**

Type of names assigned to the CA and to the Subscriber is described in the relevant Certificate Profile documentation publish in ADACOM's repository

ADACOM CA and Subscriber Certificates contain X.501 Distinguished Names in the Issuer and Subject fields.

#### **3.1.2 Need for Names to be Meaningful**

Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate. ADACOM CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

#### **3.1.3 Anonymity or Pseudonymity of Subscribers**

Not applicable.



### **3.1.4 Rules for Interpreting Various Name Forms**

No stipulation.

### **3.1.5 Uniqueness of Names**

ADACOM ensures that Subject Distinguished Names (DN) of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. The uniqueness of the Distinguished Name for electronic signatures and authentication is ensured by the Serial Number attribute value in the Subject field of the certificate. For electronic seals is ensured by the Organizational Identifier attribute value in the Subject field of the certificate.

### **3.1.6 Recognition, Authentication, and Role of Trademarks**

Certificate applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. ADACOM, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. ADACOM is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

## **3.2 Initial Identity Validation**

### **3.2.1 Method to Prove Possession of Private Key**

The Certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration or another ADACOM and Symantec approved method. This requirement does not apply where a key pair is generated by ADACOM on behalf of a Subscriber, for example where pre-generated keys are placed on QSCD.

### **3.2.2 Authentication of Organization identity**

The legal person's identity who is the Subject and/or the Subscriber of an EU Qualified Certificate is verified pursuant to current legislation and the following requirements:

i) by the physical presence of an authorized representative of the legal person who submits to an ADACOM's RA or an LRA's authorized employee the following documents:

- Proof of the Subscriber's identity [full name, date and place of birth] on the basis of a National ID (for Greece and Cyprus) or Passport issued by any other country, given that the document includes a unique number assigned to the applicant by the above mentioned identity document issuing country. The attestation of the National ID or Passport must be in the Greek, English, French or German language. In case of a National ID or Passport issued in other than the above languages, the attestation must be accompanied by an official translation in one of the above mentioned languages. ADACOM's RA or LRA's employee shall make a photocopy of the submitted identity document, which must be signed by the Subscriber and the authorized ADACOM's RA or an LRA employee;

- Proof of full name and legal status of the legal entity on the basis of certified copies of organizational documents evidencing the official registration, the existence and operation of the legal person at the time of submission, issued not more than thirty (30) days before;
- Proof of representative's authorization to represent the legal person for the issuance of the specific EU Qualified Certificate on the basis of certified copies of related corporate documents.

OR

ii) by sending all the aforementioned documents in dully certified or notarized copies via courier or postal service to ADACOM's RA office. Certification or notarization of documents' copies is provided by a notary public, legal counsel or other official with comparable authority within the subscriber's/subject's jurisdiction.

The attestation of the above documents must be in the Greek, English, French or German language. In case of documents issued in other than the above languages, the attestation must be accompanied by an official translation in one of the above mentioned languages.

### **3.2.3 Authentication of Individual Identity**

The natural person's identity who is the Subscriber and/or the Subject of an EU Qualified Certificate is verified pursuant to current legislation and the following requirements:

1. In case of a natural person who is the Subscriber and the Subject of a EU Qualified Certificate:
  - i) by the physical presence of the natural person who submits to an ADACOM's RA or an LRA's authorized employee the following documents: Proof of the Subscriber's identity [full name, date and place of birth] on the basis of a National ID (for Greece and Cyprus) or Passport issued by any other country, given that the document includes a unique number assigned to the applicant by the above mentioned identity document issuing country. The attestation of the National ID or Passport must be in the Greek, English, French or German language. In case of a National ID or Passport issued in other than the above languages, the attestation must be accompanied by an official translation in one of the above mentioned languages. ADACOM's RA or LRA's employee shall make a photocopy of the submitted identity document, which must be signed by the Subscriber and the authorized ADACOM's RA or LRA's employee;
  - ii) by the physical presence of a dully authorized representative of the Subscriber provided that the representative is duly mandated by the Subscriber to represent him/her;
  - iii) by sending all the aforementioned documents in dully certified or notarized copies via courier or postal service to ADACOM's RA office. Certification or notarization of documents' copies is provided by a notary public, legal counsel or other official with comparable authority within the subscriber's/subject's jurisdiction
  - iv) by equivalent to physical presence by Remote ID verification by which the natural person is identified through a live video call session by an authorized LRA employee. The natural person shall provide proof of his/her National ID (for Greece and Cyprus) or Passport issued by any other country, given that the document includes a unique number assigned to the applicant by the above mentioned identity document issuing country.
2. In case of a natural person who is the Subject of a EU Qualified Certificate associated with a Subscriber who is a legal person:

i) by the physical presence of the natural person associated with legal person who submits to an ADACOM's RA or an LRA's authorized employee the following documents:

- Proof of the Subscriber's identity [full name, date and place of birth] on the basis of a National ID (for Greece and Cyprus) or Passport issued by any other country, given that the document includes a unique number assigned to the applicant by the above mentioned identity document issuing country. The attestation of the National ID or Passport must be in the Greek, English, French or German language. In case of a National ID or Passport issued in other than the above languages, the attestation must be accompanied by an official translation in one of the above mentioned languages;
- Proof of the affiliation of the natural person to the legal person consistent with national or other applicable identification practices;
- Written and dully signed approval by the legal person and the natural person that the subject attributes also identify such organization.

ii) by sending all the aforementioned documents in dully certified or notarized copies via courier or postal service to ADACOM's RA office. Certification or notarization of documents' copies is provided by a notary public, legal counsel or other official with comparable authority within the subscriber's/subject's jurisdiction.

iii) by the physical presence of a dully authorized representative of the Subscriber provided that the representative is duly mandated by the Subscriber to represent him/her.

In case the individual requesting the Certificate is an RA or LRA authorized employee, the identity validation of this very individual must not be conducted by herself/himself and must involve one of her/his RA/LRA peers.

### **3.2.4 Non-Verified Subscriber information**

Non-verified subscriber information includes:

- Organization Unit (OU) attributes
- Any other information designated as non-verified in the Certificate

### **3.2.5 Validation of Authority**

Whenever a natural person's name is associated with a legal person's name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the legal person ADACOM's RA:

- Determines that the legal person exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the legal person, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the legal person, the employment with the legal person of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the legal person.

### **3.2.6 Criteria for Interoperation**

- No stipulation.

## ***3.3 Identification and Authentication for Re-key Requests***

Prior to the expiration of an existing EU Qualified Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. ADACOM generally requires

that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as “rekey”).

Please refer to Sections 3.2.2 and 3.2.3 of this CPS.

In addition, all documents required can be sent electronically digitally signed by an existing EU Qualified Certificate for electronic signatures.

### **3.3.1 Identification and Authentication for Routine Re-key**

Not applicable

### **3.3.2 Identification and Authentication for Re-key After Revocation**

Refer to Sections 3.2.2 and 3.2.3 of this CPS.

## ***3.4 Identification and Authentication for Revocation Request***

Prior to the revocation of a Certificate, ADACOM verifies that the revocation has been requested by the Certificate’s Subscriber, the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include one or more of the following:

- Having the Subscriber submit the Subscriber’s Challenge Phrase and revoking the Certificate automatically if it matches the Challenge Phrase on record
- Receiving a message from the Subscriber that requests revocation and contains a qualified electronic signature verifiable with reference to the Certificate to be revoked
- Communication with the Subscriber providing reasonable assurances, that the natural or legal person requesting revocation is, in fact the Subscriber or has the duly authorization to do so. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

ADACOM RA Administrators are entitled to request the revocation of Certificates. ADACOM authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

## **4. CERTIFICATE LIFE-CYCLE OPERATIONAL**

### ***4.1 Certificate Application***

#### **4.1.1 Who Can Submit a Certificate Application?**

Application for EU Qualified Certificates may be submitted by a natural or legal person, who is the Subscriber of the Certificate, provided that is legally eligible.

#### **4.1.2 Enrollment Process and Responsibilities**

All Certificate Subscribers shall manifest assent to the relevant General Terms and Conditions that contain representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- Accept the Terms and Conditions regarding the use of the certificate

- Completing and signing a Certificate Application and Agreement form by providing true and correct information in accordance with the requirements of this policy
- Provide relevant validation documents
- Generating, or arranging to have generated, a key pair
- Receiving his, her, or its certificate, directly or through the RA,
- Demonstrating possession and/or exclusive control of the private key corresponding to the public key.

## **4.2 Certificate Application Processing**

### **4.2.1 Performing Identification and Authentication Functions**

ADACOM performs identification and authentication of all required Subscriber information in terms of Section 3.2.

### **4.2.2 Approval or Rejection of Certificate Applications**

ADACOM approves an application for a certificate only if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment has been received

ADACOM rejects a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- ADACOM believes that issuing a certificate to the Subscriber may bring ADACOM into disrepute.

Upon certificate application rejection, Subscriber has the right either to return the QSCD in accordance to Section 9.1.5 or to keep it for future usage under his own full responsibilities.

In case ADACOM rejects a certificate application related to a Remote QSCD, the relevant Subscriber account is not created and no other actions are needed from Subscriber

### **4.2.3 Time to Process Certificate Applications**

ADACOM begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant General Terms and Conditions, CPS or other agreement. A certificate application remains active until the enrollment procedure is completed, which cannot exceed one (1) month from the date of submission of the Application Form for Certificate issuance.

## **4.3 Certificate Issuance**

### **4.3.1 CA Actions during Certificate Issuance**

A Certificate is created and issued following the approval of a Certificate Application by ADACOM. ADACOM creates and issues to a Certificate Subscriber a Certificate based on the information in a Certificate Application following approval of such Certificate Application. In order for the Application to be approved, the Subscriber must provide the identification documents defined in the Application Form for Certificate issuance. These identification documents shall be

accepted only if they are duly validated by the competent authorities no more than six (6) months before the submission of the Application Form.

#### **4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate**

ADACOM notifies Subscribers that they have created such Certificates, and provides Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates are made available to Subscribers, by informing them via an e-mail message.

### **4.4 Certificate Acceptance**

#### **4.4.1 Conduct Constituting Certificate Acceptance**

The following conduct constitutes certificate acceptance:

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

#### **4.4.2 Publication of the Certificate by the CA**

ADACOM publishes the Certificates it issues in a publicly accessible repository.

#### **4.4.3 Notification of Certificate Issuance by the CA to Other Entities**

RAs and LRAs may receive notification of the issuance of certificates they approve.

### **4.5 Key Pair and Certificate Usage**

#### **4.5.1 Subscriber Private Key and Certificate Usage**

Use of the private key corresponding to the public key in the Certificate is only permitted once the Subscriber has agreed to the General Terms and Conditions, accepted the Certificate. The Certificate shall be used lawfully in accordance with ADACOM's General Terms and Conditions, the terms of the STN CP and this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the Certificate.

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key.

#### **4.5.2 Relying Party Public Key and Certificate Usage**

Relying parties shall assent to ADACOM's General Terms and Conditions as a condition of relying on the Certificate.

Reliance on a Certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

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

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

#### **4.6 Certificate Renewal**

Not applicable.

#### **4.7 Certificate Re-Key**

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

##### **4.7.1 Circumstances for Certificate Re-Key**

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

##### **4.7.2 Who May Request Certification of a New Public Key**

Only the Subscriber may request Certificate re-keying.

##### **4.7.3 Processing Certificate Re-Keying Requests**

Re-keying procedures ensure that the Subscriber seeking to re-key a Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

The Subscriber submits a re-keying application to ADACOM RA or to an LRA and ADACOM RA or the LRA, reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements, as described in Section 3.3.1.

Other than this procedure or another ADACOM -approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

#### **4.7.4 Notification of New Certificate Issuance to Subscriber**

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

#### **4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate**

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

#### **4.7.6 Publication of the Re-Keyed Certificate by the CA**

The re-keyed certificate is published in ADACOM's publicly accessible repository.

#### **4.7.7 Notification of Certificate Issuance by the CA to Other Entities**

RAs and LRAs may receive notification of the issuance of Certificates they approve.

### **4.8 *Certificate Modification***

#### **4.8.1 Circumstances for Certificate Modification**

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

#### **4.8.2 Who May Request Certificate Modification**

See Section 4.1.1.

#### **4.8.3 Processing Certificate Modification Requests**

ADACOM performs identification and authentication of all required Subscriber information in terms of Section 3.2.

#### **4.8.4 Notification of New Certificate Issuance to Subscriber**

See Section 4.3.2.

#### **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

See Section 4.4.1.

#### **4.8.6 Publication of the Modified Certificate by the CA**

See Section 4.4.2.

#### **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

See Section 4.4.3.



## **4.9 Certificate Revocation and Suspension**

### **4.9.1 Circumstances for Revocation**

The ADACOM's General Terms and Conditions provide the obligation and/or right of the Subscriber to request revocation of a Certificate. Only in the circumstances listed below, will a Subscriber Certificate be revoked by ADACOM (or by the Subscriber) and published on a CRL.

A Subscriber Certificate is revoked if:

- ADACOM or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key. In case a compromise is reported by a third party ADACOM requires respective confirmation from the Subscriber.
- ADACOM has reason to believe that the Subscriber has breached a material obligation, representation, or warranty under the applicable General Terms and Conditions for Use of EU Qualified Certificates,
- ADACOM has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CPS, was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate,
- ADACOM has reason to believe that a material fact in the Certificate Application is false,
- ADACOM determines that a material prerequisite to Certificate issuance was neither satisfied nor waived,
- Subscriber loses the legal eligibility, is declared in absence or death, is dissolved or declared bankrupted, taking into consideration that each certificate is non-transferable in any case,
- Subscriber loses ability to use the local QSCD or mobile device required to access a remote QSCD
- In case the Subject of the Certificate is a natural person associated with the Subscriber-legal person and the Subscriber requires the revocation.
- A final court judgment requires the relevant revocation or cancellation
- The private key of the CA has been compromised.
- The Supervisory Body requests the revocation according to the law
- The Subscriber identity has not been successfully re-verified
- The Subscriber has not submitted payment, when due
- The continued use of that certificate is harmful to ADACOM and/or STN.

When considering whether Certificate usage is harmful to ADACOM and/or STN, ADACOM considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

ADACOM may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

ADACOM General Terms and Conditions for Use of EU Qualified Certificates require Subscribers to immediately notify ADACOM of a known or suspected compromise of its private key.

After the approval of a revocation request by the CA, the revoked certificate cannot be re-entered into force.

### **4.9.2 Who Can Request Revocation**

Request for revocation of an EU Qualified Certificate may be submitted by:

- RA or LRA
- a natural or legal person, or their legal representatives, who is the Subscriber of the Certificate, or a successor who wishes to request revocation in case of a deceased Subscriber (natural person), provided that is legally eligible
- a competent court or authority
- the Supervisor Body

Request for revocation of a CA Certificate may be submitted by:

- a legal person, who is the Subscriber of the Certificate, provided that is legally eligible,
- a competent court or authority
- the Supervisor Body

### **4.9.3 Procedure for Revocation Request**

#### **Procedure for Requesting the Revocation of a Subscriber Certificate**

A Subscriber or Subscriber's successor who wishes to request revocation is required to send a request to ADACOM either by e-mail at [revoke@adacom.com](mailto:revoke@adacom.com) or communicate by telephone at +30 210 9577255, or, alternatively, via ADACOM's Self Service Web Portal. ADACOM will promptly initiate revocation of the certificate.

Communication of such revocation request shall be in accordance with Section 3.4.

In case of Short-lived Certificate, revocation by Subscriber is not available.

### **4.9.4 Revocation Request Grace Period**

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

### **4.9.5 Time within Which CA Must Process the Revocation Request**

ADACOM takes commercially reasonable steps to process revocation requests without delay and in any case the maximum delay from the time ADACOM receives a revocation request in accordance with Section 4.9.3 and the decision to change its status information being available to all relying parties shall be at most 24 hours. If though the revocation request cannot be confirmed within 24 hours then the status need not be changed.

Right after the approval of a revocation request, the CA informs the Subscriber and the Subject of the certificate for the revocation via e-mail for this event.

### **4.9.6 Revocation Checking Requirements for Relying Parties**

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement by checking Certificate status using the ADACOM web-based repository or by using OCSP. CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository or OCSP responder to check for revocation status. Due to the numerous and varying locations for CRL repositories, relying parties are advised to access CRLs using the URL(s) embedded in a certificate's CRL Distribution Points extension.

The proper OCSP responder for a given certificate is placed in its Authority Information Access extension.

#### **4.9.7 CRL Issuance Frequency**

CRLs for Subscriber Certificates are issued at least once per day. CRLs for CA Certificates are issued at least annually, but also whenever a CA Certificate is revoked. ADACOM shall not remove from the CRL revoked certificates after they have expired.

#### **4.9.8 Maximum Latency for CRLs**

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

#### **4.9.9 On-Line Revocation/Status Checking Availability**

Online revocation and other Certificate status information are available via a web-based repository and OCSP. In addition to publishing CRLs, ADACOM provides Certificate status information through query functions in the ADACOM repository.

Certificate status information for EU Qualified Certificates is available at the ADACOM Repository at: <https://pki.adacom.com/repository>

The maximum delay between the confirmation of the revocation of a certificate to become effective and the actual change of the status information of this certificate being made available to relying parties is at most 60 minutes. If though the revocation request requires revocation in advance (e.g. Subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the confirmation time.

#### **4.9.10 On-Line Revocation Checking Requirements**

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the ADACOM repository or by requesting Certificate status using the applicable OCSP responder.

#### **4.9.11 Other Forms of Revocation Advertisements Available**

Not applicable.

#### **4.9.12 Special Requirements regarding Key Compromise**

ADACOM uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of its own CAs.

#### **4.9.13 Circumstances for Suspension**

Not applicable.

#### **4.9.14 Who Can Request Suspension**

Not applicable.

#### **4.9.15 Procedure for Suspension Request**

Not applicable.

#### **4.9.16 Limits on Suspension Period**

Not applicable.

### ***4.10 Certificate Status Services***

#### **4.10.1 Operational Characteristics**

The Status of public certificates is available via CRL, LDAP directory and an OCSP responder.

#### **4.10.2 Service Availability**

ADACOM shall ensure that its Certificate Status Services are available 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 0.1% annually.

#### **4.10.3 Optional Features**

Not applicable.

### ***4.11 End of Subscription***

A Subscriber may end a subscription for an ADACOM EU Qualified Certificate by:

- Allowing the EU Qualified Certificate to expire without re-keying that Certificate,
- Revoking the EU Qualified Certificate before Certificate expiration without replacing it

### ***4.12 Key Escrow and Recovery***

Not applicable.

#### **4.12.1 Key Escrow and Recovery Policy and Practices**

Not applicable.

#### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

Not applicable.

## **5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

### ***5.1 Physical Controls***

ADACOM has implemented the ADACOM Physical Security Policy which supports the security requirements of this CPS. Compliance with these policies is included in ADACOM's audit requirements described in section 8. ADACOM Physical Security Policy contains sensitive

security information and is only available upon agreement with ADACOM. An overview of the requirements is described below.

### **5.1.1 Site Location and Construction**

ADACOM CA and RA 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 CA operations. ADACOM's Disaster Recovery facilities are protected by multiple tiers of physical security comparable to those of ADACOM's primary facility.

### **5.1.2 Physical Access**

ADACOM CA 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 CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, 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 RA 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 RA operations in secure containers.

ADACOM securely stores the Cryptographic Signing Units (CSU) used to generate and store the Subscribers Private Keys for remote signature. Access to the rooms used for key storage and key generation activities is controlled and logged by the building access card system. Access card logs and video records are reviewed on a regular basis.

### **5.1.3 Power and Air Conditioning**

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.

#### **5.1.4 Water Exposures**

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

#### **5.1.5 Fire Prevention and Protection**

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.

#### **5.1.6 Media Storage**

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).

#### **5.1.7 Waste Disposal**

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with ADACOM's normal waste disposal requirements.

#### **5.1.8 Off-Site Backup**

ADACOM performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using the secure off-site Disaster Recovery facility in accordance with "ADACOM Disaster Recovery Plan".

### **5.2 Procedural Controls**

#### **5.2.1 Trusted Roles**

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

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

Trusted Persons include, but are not limited to:

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

ADACOM considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

### **5.2.2 Number of Persons Required per Task**

ADACOM has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold "Secret Shares" and vice versa.

### **5.2.3 Identification and Authentication for Each Role**

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 in Section 5.3.2.

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, RA, 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.

### **5.2.4 Roles Requiring Separation of Duties**

Roles requiring Separation of duties include, but are not limited to:

- The validation and handling of information in Certificate Applications;

- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or re-keying requests, or enrollment information;
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- The generation, issuing or destruction of a CA certificate;
- The loading of a CA to a Production environment.
- The access to the Remote QSCD

### **5.3 Personnel Controls**

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

#### **5.3.1 Qualifications, Experience, and Clearance Requirements**

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 and - 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.

#### **5.3.2 Background Check Procedures**

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.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person;
- Highly unfavorable or unreliable professional references;



- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable laws.

### **5.3.3 Training Requirements**

ADACOM provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. ADACOM maintains records of such training. ADACOM periodically reviews and enhances its training programs as necessary.

ADACOM's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- ADACOM security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

### **5.3.4 Retraining Frequency and Requirements**

ADACOM provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

### **5.3.5 Job Rotation Frequency and Sequence**

No rotation used.

### **5.3.6 Sanctions for Unauthorized Actions**

Appropriate disciplinary actions are taken (as part of ADACOM Security Policy) for unauthorized actions or other violations of ADACOM policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

### **5.3.7 Independent Contractor Requirements**

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to ADACOM employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in Section 5.3.2 are permitted access to ADACOM 's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

### **5.3.8 Documentation Supplied to Personnel**

ADACOM provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

## **5.4 Audit Logging Procedures**

### **5.4.1 Types of Events Recorded**

ADACOM ensures that all relevant information concerning the operation of the Trust Services is recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of the Trust Service operation.

ADACOM manually or automatically logs the following significant events:

- CA certificate and key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Changes to CA details or keys
  - Cryptographic device life cycle management events.
- Subscriber certificate and key life cycle management events, including:
  - Certificate Applications, issuance, re-key, and revocation
  - Key generation, backup, storage, recovery, archival, and destruction
  - Successful or unsuccessful processing of requests
  - Changes to certificate creation policies
  - Generation and issuance of Certificates and CRLs.
- Trusted Employee Events, including:
  - Logon and logoff attempts
  - Attempts to create, remove, set passwords or change the system privileges of any privileged users
  - Personnel changes.
- All significant security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - Start-up and shutdown of systems and applications
  - Possession of activation data for CA private key operations
  - System configuration changes and maintenance
  - PKI and security system actions performed by ADACOM personnel
  - Security sensitive files or records read, written or deleted
  - Security policy settings changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit.
  - Remote QSCD facility access entry/exit

Log entries include the following elements:

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

ADACOM RA and LRA log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant

- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's identification card number) of identification documents, if applicable. Storage location of copies of applications and identification documents for EU Qualified Certificates
- Any specific choices in the Certificate Application
- Identity of entity accepting the application and in case of EU Qualified e-Seals identity of the natural person representing the legal person to whom the EU Qualified Certificate for the electronic seal is provided
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA and LRA, if applicable.

#### **5.4.2 Frequency of Processing Log**

ADACOM systems are continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

#### **5.4.3 Retention Period for Audit Log**

Audit logs shall be retained for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.

Physical or digital archive records about certificate applications, registration information and requests or applications for revocation are retained for at least seven (7) years after any certificate based on these records ceases to be valid.

In case of CA termination ADACOM audit logs and archive records are retained and accessible until abovementioned term for retention in accordance with Section 5.8.

#### **5.4.4 Protection of Audit Log**

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

#### **5.4.5 Audit Log Backup Procedures**

Incremental backups of audit logs are created daily and full backups are performed weekly.

#### **5.4.6 Audit Collection System (Internal vs. External)**

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by ADACOM personnel in Trusted Roles.

#### **5.4.7 Notification to Event-Causing Subject**

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

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

#### **5.4.8 Vulnerability Assessments**

Events in the audit process are logged, in part, to monitor system vulnerabilities. Vulnerability Assessments are performed, reviewed, and revised. An annual Vulnerability Assessment will be an input into ADACOM's annual audit.

### **5.5 Records Archival**

#### **5.5.1 Types of Records Archived**

ADACOM archives:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information

#### **5.5.2 Retention Period for Archive**

The retention period for archive is described in Section 5.4.3.

#### **5.5.3 Protection of Archive**

ADACOM protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

#### **5.5.4 Archive Backup Procedures**

ADACOM incrementally backs up electronic archives on a daily basis and performs full backups on a weekly basis. Electronic copies of paper-based records are maintained on ADACOM's off-site secure facility.

#### **5.5.5 Requirements for Time-Stamping of Records**

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

#### **5.5.6 Archive Collection System (Internal or External)**

ADACOM uses an internal archive collection system.

#### **5.5.7 Procedures to Obtain and Verify Archive Information**

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

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

## **5.6 Key Changeover**

ADACOM CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. ADACOM CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs are generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). ADACOM's CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

## **5.7 Compromise and Disaster Recovery**

### **5.7.1 Incident and Compromise Handling Procedures**

Backups of the following CA information are kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys are generated and maintained in accordance with this CPS.

### **5.7.2 Computing Resources, Software, and/or Data Are Corrupted**

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to ADACOM Security and ADACOM's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, ADACOM's key compromise or disaster recovery procedures will be enacted.

### **5.7.3 Entity Private Key Compromise Procedures**

Upon the suspected or known Compromise of an ADACOM CA, ADACOM follows the plan of actions as described within Security Incident Management procedure.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the ADACOM repository in accordance with Section 4.9.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected Participants, and

- The CA will generate a new key pair in accordance with Section 5.6, except where the CA is being terminated in accordance with Section 5.8.

This paragraph is also applicable in case PKI algorithms or associated parameters become insufficient for its remaining intended usage.

#### **5.7.4 Business Continuity Capabilities after a Disaster**

ADACOM maintains a Business Continuity Plan (BCP) in order to establish procedures to recover the ADACOM critical business functions following a disaster.

The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - Notification/Activation phase to detect and assess damage and activate the plan.
  - Recovery phase to restore temporary IT operations and recover damage done to the original system.
- Identify the activities, resources, and procedures needed to carry out ADACOM CA and Certificate functions during prolonged interruptions to normal operations.
- Assign responsibilities to designated ADACOM personnel and provide guidance for recovering ADACOM procedures during prolonged periods of interruption to normal operations.
- Ensure coordination with other ADACOM staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

ADACOM has the capability to restore or recover essential operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- Publication of revocation information.

ADACOM maintains redundant hardware and backups of its CA and infrastructure system software at its Disaster Recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with Section 6.2.4.

### **5.8 CA or RA Termination**

The CA is terminated:

- with a decision of the ADACOM's Board of Directors;
- 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 CA, to cease operation, ADACOM makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, ADACOM will activate the documented "ADACOM Termination Plan" to minimize disruption to Customers, Subscribers, and Relying Parties. This termination plan may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by ADACOM,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key, including backup key, and the hardware tokens containing such private key,
- Provisions needed for the transition of the CA's services to a successor CA where possible,
- Provision notice to relevant authorities such as supervisory bodies,
- Transfer of obligations to a reliable party for maintaining all information necessary to provide evidence of the Trust Services operation for a reasonable period, unless it can be demonstrated that ADACOM does not hold such information,
- The submission of the ADACOM CA's archives and records to another contracting Certification Service Provider for EU Qualified Certificates, for the time periods required by the law.

## **6. TECHNICAL SECURITY CONTROLS**

### **6.1 *Key Pair Generation and Installation***

#### **6.1.1 Key Pair Generation**

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. The cryptographic modules used for key generation meet the requirements of FIPS 140-2 level 3.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the Symantec Security and Audit Requirements Guide. The activities performed in each key generation ceremony 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.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. The Subscriber uses a QSCD certified cryptographic module compliant with eIDAS Regulation requirements.

For EU Remote Qualified Certificates, the generation of keys, their storage and subsequent use, is performed by ADACOM using exclusively devices certified specifically in accordance with the applicable requirements per Article 30.3 of the eIDAS and, thus included in the list of qualified devices maintained by the European Commission in compliance with Articles 30, 31 and 39 of eIDAS.

#### **6.1.2 Private Key Delivery to Subscriber**

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

When Subscriber key pairs are pre-generated by ADACOM on QSCD, such device is delivered to the Subscriber using a commercial registered mail delivery service. The data required to activate the device is communicated to Subscriber using an out of band process. The distribution of such devices is monitored by ADACOM.

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

When Subscriber key pairs are generated on a remote QSCD by the Subscriber, private key delivery to the Subscriber is performed inside the remote QSCD.

#### **6.1.3 Public Key Delivery to Certificate Issuer**

Subscribers submit their public key to ADACOM for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where Subscriber key pairs are pre-generated by ADACOM, this requirement is not applicable.



### **6.1.4 CA Public Key Delivery to Relying Parties**

ADACOM makes the Root CA Certificates available to Subscribers and Relying Parties through their inclusion in web browser software. As new Root CA Certificates are generated, Symantec provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

ADACOM generally provides its own full certificate chain (including the issuing CA and any CAs in the chain) to the Subscriber upon Certificate issuance.

Subscribers, during the certificate pick-up process, automatically download and install into their computer, the intermediate and issuing CA's public keys. In any case if a user needs to verify and/or download the public key of the CA, he can do so by accessing the ADACOM's web-based repository (<https://pki.adacom.com/repository>).

### **6.1.5 Key Sizes**

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The ADACOM Standard for minimum key sizes is the use of key pair equivalent in strength to minimum 2048 bit RSA for CAs and Subscriber certificates

All CAs and Subscriber certificates use SHA-256 for digital signature hash algorithm.

### **6.1.6 Public Key Parameters Generation and Quality Checking**

The quality of Public Keys is guaranteed by using secure random number generators built into the QSCD.

### **6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)**

Refer to Section 7.

## ***6.2 Private Key Protection and Cryptographic Module Engineering Controls***

ADACOM has implemented a combination of physical, logical, and procedural controls to ensure the security of ADACOM CA private keys. Subscribers are also required to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

### **6.2.1 Cryptographic Module Standards and Controls**

For CA key pair generation and CA private key storage, ADACOM uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-2 Level 3.

Subscriber Private Keys are generated on QSCD compliant to eIDAS Regulation requirements.

ADACOM monitors QSCD certification status until the end of the validity period of the certificate associated with the relevant QSCD. In case of a modification of the certification status of the QSCD, ADACOM will stop issuing certificates on these devices.

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

ADACOM has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. ADACOM uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and trusted individuals called “Shareholders.” A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is three (3). It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

No Multi-Person control is applied to Subscriber Private keys.

### **6.2.3 Private Key Escrow**

ADACOM CA and Subscribers private keys are not escrowed.

### **6.2.4 Private Key Backup**

ADACOM creates backup copies of CA private keys and Subscriber private keys generated and stored by a Remote QSCD, for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for private key storage meet the requirements of this CPS. Private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing onsite backup copies of CA private keys are subject to the requirements of this CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

In case of a local QSCD the Subscriber Private Keys cannot be extracted or restored from the QSCD and are not backed up.

### **6.2.5 Private Key Archival**

Upon expiration of an ADACOM CA Certificate, the key pair associated with the certificate is securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CPS. These CA key pairs are not used for any signing events after their expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CPS.

The Subscriber Private Keys cannot be extracted or restored from the QSCD and are not archived.

### **6.2.6 Private Key Transfer Into or From a Cryptographic Module**

ADACOM generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, ADACOM makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

ADACOM generates Subscriber key pairs on the hardware cryptographic modules in which the keys will be used. In addition, ADACOM makes copies of such Subscriber key pairs for high availability and disaster recovery purposes. Where Subscriber key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

### **6.2.7 Private Key Storage on Cryptographic Module**

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

### **6.2.8 Method of Activating Private Key**

All ADACOM Subscribers shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

Activation data generation is described in Section 6.4.1

The Subscriber Private Keys on Local QSCD are protected by PIN codes. The following rules apply:

- Subscriber needs to enter the PIN code to the QSCD for each transaction.
- Subscriber is obligated to change the PIN and PUK code prior the initial registration process
- In case the Subscriber enters a wrong PIN code 5 times in a row, the QSCD is blocked
- PIN can be unblocked using an admin PIN code
- The usage of admin PIN code will be blocked after 3 consecutive incorrect tries
- User can change the PIN and PUK codes.

The Subscriber Private Keys on Remote QSCD are protected by username, password and OTP codes. The following rules apply:

- Subscriber needs to enter the username, password and OTP code to the QSCD for each transaction.
- In case the Subscriber enters a wrong username, password and OTP code 5 times in a row, the Remote QSCD account is locked
- Remote QSCD account cannot be password reset
- User can change the password.

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

### **6.2.9 Method of Deactivating Private Key**

ADACOM CA private keys are deactivated upon power off of the cryptographic module.

Subscriber private keys may be deactivated after each operation, upon logging off their system, upon removal of the Local QSCD from the system, or upon logging off of the Remote QSCD. In all cases, Subscribers have an obligation to adequately protect their private key(s) in accordance with this CPS.

### 6.2.10 Method of Destroying Private Key

Where required, ADACOM destroys CA and Subscriber private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. ADACOM utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, key destruction activities are witnessed.

The Subscriber Private Keys of a Local QSCD can be destroyed by physically destroying or damaging the QSCD.

### 6.2.11 Cryptographic Module Rating

See Section 6.2.1.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

ADACOM CA, RA and Subscriber Certificates are backed up and archived as part of ADACOM's routine backup procedures.

All the Subscriber Public Keys are kept in database of ADACOM and may be archived for at least seven (7) years after expiration of the CA that has issued the certificates.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for signature verification. The maximum Operational Periods for ADACOM Certificates issued on or after the effective date of this CPS are set forth in the following table below.

<b><i>Certificate Issued By:</i></b>	<b><i>Validity Period</i></b>
PCA Root CA	Normally up to 30 years
ADACOM Issuing CA	Normally up to 8 years
Subscriber Long-lived Certificate	Normally 1-3 years
Subscriber Short-lived Certificate	Normally up to 24 hours

In addition, ADACOM CAs stop issuing new Certificates at an appropriate date (60 days plus maximum validity period of issued Certificates) prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Subscribers shall cease all use of their key pairs after their usage periods have expired.

If an algorithm or the appropriate key length offers no sufficient security during the validity period of the certificate, the concerned certificate will be revoked and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by the ADACOM management.

## **6.4 Activation Data**

### **6.4.1 Activation Data Generation and Installation**

Activation data (Secret Shares) used to protect HSM containing ADACOM CA private keys are generated in accordance with the requirements of Section 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

Activation data used (PINs) to protect Local QSCD containing Subject's private keys are generated in accordance with the user manual of the QSCD.

- Where Subscriber key pairs are pre-generated by ADACOM, activation data are delivered to the Subscriber using a commercial registered mail delivery service.
- Where Subscriber key pairs are generated by the Subscriber, pre-defined activation data must be changed immediately before the key generation.

Activation data used (username, password and OTP code) to protect Remote QSCD containing Subject's private keys are generated in accordance with the compliance requirements of the QSCD.

### **6.4.2 Activation Data Protection**

ADACOM Shareholders are required to safeguard their Secret Shares and remote QSCD Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

The Subscriber shall memorize the activation credentials (PIN, PUK, username, password, OTP) and not share them with anyone else.

### **6.4.3 Other Aspects of Activation Data**

#### **6.4.3.1 Activation Data Transmission**

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

#### **6.4.3.2 Activation Data Destruction**

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

## **6.5 Computer Security Controls**

ADACOM performs all CA and RA functions using trustworthy systems that meet the requirements of ADACOM ISMS and Symantec's Security and Audit Requirements Guide.

### **6.5.1 Specific Computer Security Technical Requirements**

ADACOM ensures that the systems maintaining CA software and data files are trustworthy systems secure from unauthorized access. 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.

ADACOM's production network is logically separated from other components. This separation prevents network access except through defined application processes. ADACOM uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

All critical software components are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorized software.

ADACOM personnel are authenticated before using critical applications related to the services. User accounts are created for personnel in specific roles that need access to the system in question. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

ADACOM requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. ADACOM requires that passwords be changed on a periodic basis.

Direct access to ADACOM databases supporting ADACOM's CA Operations is limited to Trusted Persons having a valid business reason for such access.

The ADACOM certification services system components are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that change must be approved by the Security Officer. The approval is documented for further reference.

All media containing production environment software and data, audit, archive, or backup information are stored within ADACOM with appropriate physical and logical access controls. Media containing Sensitive Information are securely disposed of when no longer required.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

## **6.5.2 Computer Security Rating**

No stipulation.

## **6.6 Life Cycle Technical Controls**

### **6.6.1 System Development Controls**

New versions of software are developed and implemented in accordance to change management procedure.

New or updated software, when first loaded provides a method to verify that the software on the system originated from trust source, has not been modified prior to installation, and is the version intended for use.

## **6.6.2 Security Management Controls**

ADACOM has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. Symantec creates a hash of all software packages and Symantec software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, ADACOM validates the integrity of its CA systems. Only the software directly used for performing the tasks is used in the information system.

## **6.6.3 Life Cycle Security Controls**

ADACOM policies and assets are reviewed at planned intervals, or when significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

The configurations of ADACOM systems are checked at least annually for changes that violate the ADACOM security policies. Changes that have an impact on the level of security provided are reviewed by the Security Officer and approved by the Management.

ADACOM has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

ADACOM manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment.

## **6.7 Network Security Controls**

ADACOM performs all its CA and RA functions using networks secured in accordance with the ADACOM ISMS and Symantec Security and Audit Requirements Guide to prevent unauthorized access and other malicious activity. ADACOM protects its communications of sensitive information through the use of encryption and digital signatures.

The security level of the internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

ADACOM performs a vulnerability assessment periodically on public and private IP addresses as long as penetration tests on the certification systems.

## **6.8 Time-Stamping**

Certificates, CRLs, and other revocation database entries contain time and date information.

# **7. CERTIFICATE, CRL, AND OCSP PROFILES**

## **7.1 Certificate Profile**

Certificate profile is in accordance with the X.509 version 3, the IETF RFC 5280 and clause 6.6.1 of ETSI EN 319 411-1.

Certificates profiles are published in ADACOM's public repository <https://pki.adacom.com/repository/en/profiles>.

## **7.2 CRL Profile**

CRL profile is in accordance with the X.509 version 2 and the IETF RFC 5280.  
CRL profiles are published in ADACOM's public repository <https://pki.adacom.com/repository/en/profiles>.

## **7.3 OCSP Profile**

OCSP profile is in accordance with the IETF RFC 6960.  
OCSP profiles are published in ADACOM's public repository <https://pki.adacom.com/repository/en/profiles>.

# **8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

The conformity of information system, policies and practices, facilities, personnel, and assets of ADACOM are assessed by a conformity assessment body pursuant to the eIDAS regulation, the corresponding legislation and standards or whenever a major change is made to Trust Service operations.

In addition to compliance audits, ADACOM is entitled to perform other reviews and investigations to ensure the trustworthiness of ADACOM's Certification Services. ADACOM is entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm.

ADACOM is entitled to perform second party audits to contractors that are under a relationship with ADACOM to operate as Local Registration Authorities (LRAs).

## **8.1 Frequency and Circumstances of Assessment**

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

## **8.2 Identity/Qualifications of Assessor**

ADACOM's CA compliance audits are performed by:

- Internal Auditors,
- A conformity assessment body which is accredited in accordance with Regulation EC no 765/2008 and EN 319 403 as competent to carry out conformity assessment of Qualified Trust Service Provider and Qualified Trust Services it provides.
- The Supervisory Body

## **8.3 Assessor's Relationship to Assessed Entity**

The auditor of the conformity assessment body shall be independent from ADACOM and ADACOM's assessed systems.

The internal auditor shall not audit his/her own areas of responsibility.

## **8.4 Topics Covered by Assessment**

The conformity assessment covers the conformity of ADACOM's information system, policies and practices, facilities, personnel, and assets with eIDAS regulation, respective legislation and



standards. Conformity assessment body audits the parts of information system used to provide Trust Services.

The areas of activity subject to internal auditing are the following:

- Quality of service;
- Security of service;
- Security of operations and procedures;
- Protection of the data of Subscribers and security policy, performance of work procedures and contractual obligations, as well as compliance with the CP and service-based Policies and Practice statements.

The Conformity Assessment Body and the Internal Auditor also audit these parts of the information system, policies and practices, facilities, personnel, and the assets of sub-contractors that are related to providing ADACOM Trust Services (e.g. including LRAs).

### ***8.5 Actions Taken as a Result of Deficiency***

With respect to compliance audits of ADACOM's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by ADACOM management with input from the auditor. ADACOM management is responsible for developing and implementing a corrective action plan. If ADACOM determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the Trust Services, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, ADACOM management will evaluate the significance of such issues and determine the appropriate course of action.

Additionally, in the event of a result of the assessment by the Conformity Assessment Body, showing deficiency, the Supervisory Body requires ADACOM to remedy any failure to fulfil requirements within a time limit (if applicable) set by the Supervisory Body. ADACOM makes efforts to stay compliant and fulfil all requirements of the deficiency on time. ADACOM's management is responsible to implement a corrective action plan. ADACOM evaluates the significances of deficiencies and prioritizes appropriate actions to be taken at least during the time limit declared by Supervisory Body or reasonable period of time.

Where personal data protection rules appear to have been breached, the Supervisory Body shall inform the data protection authority of the results of the compliance audit.

### ***8.6 Communications of Results***

Audit conclusions or certificate(s) for trust service(s), which are based on audit results of the conformity assessment body conducted pursuant to the eIDAS regulation, corresponding legislation and standards, may be published on ADACOM's website <https://pki.adacom.com/repository>.

In addition ADACOM submits the resulting conformity assessment report to the Supervisory Body within at period of three (3) working days of receiving it. ADACOM submits the audit conclusions or certificate(s) for trust service(s) to maintainers of the Browsers Root Programs in which ADACOM is participating and other interested parties.

Results of the internal audits of ADACOM's operations may be released at the discretion of ADACOM Management.

## **9. OTHER BUSINESS AND LEGAL MATTERS**

### **9.1 Fees**

#### **9.1.1 Certificate Issuance or Renewal Fees**

ADACOM charges Subscribers for the issuance, management, and re-key of Certificates.

#### **9.1.2 Certificate Access Fees**

ADACOM does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

#### **9.1.3 Revocation or Status Information Access Fees**

ADACOM does not charge a fee as a condition of OCSP services and making the CRLs required by this CPS available in a repository or otherwise available to Relying Parties. ADACOM does not permit access to revocation information or certificate status information in their repositories by third parties that provide products or services that utilize such Certificate status information without ADACOM's prior express written consent.

#### **9.1.4 Fees for Other Services**

ADACOM does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with ADACOM.

#### **9.1.5 Refund Policy**

##### **9.1.5.1 Distant sales**

In case the sale of the Certificate is effected via the internet or a phone call the Subscriber has the right, under Article 4 § 10 of L. 2251/1994, as amended, to withdraw from the sales contract without stating the reasons within an exclusive time limit of fourteen (14) calendar days from the date of purchase. The exercise of this right shall be made in writing by the Subscriber to ADACOM, sending an email to [qc@adacom.com](mailto:qc@adacom.com). Subsequently, and following communication, ADACOM is obliged to repay the money corresponding to the value of the sales contract to the Subscriber. Refund payment is effected with the same method as initial payment and the Subscriber is not entitled to use the Certificate. After that period, the right of withdrawal expires and ADACOM has no further obligation for the above cause.

##### **9.1.5.2 Other cases**

Subject to Section 9.1.5.1 ADACOM handles refund case-by-case.

To request a refund Subscriber should send a written application to ADACOM. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

## **9.2 *Financial Responsibility***

### **9.2.1 Insurance Coverage**

ADACOM maintains a commercially reasonable level of civil liability insurance coverage for errors and omissions through an errors and omissions insurance program with an insurance carrier. A certificate of the insurance policy is available at the ADACOM public repository <https://pki.adacom.com/repository/en/insurance>.

### **9.2.2 Other Assets**

ADACOM has sufficient financial resources to maintain its operations and perform its duties, and is reasonably able to bear the risk of liability to Subscribers and Relying Parties. Proof of financial resources is not made publicly available.

### **9.2.3 Insurance or Warranty Coverage for End-Entities**

See Section 9.2.1 of this CPS.

## **9.3 *Confidentiality of Business Information***

### **9.3.1 Scope of Confidential Information**

All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to ADACOM because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from ADACOM about him/herself according to the applicable laws.

### **9.3.2 Information Not Within the Scope of Confidential Information**

Any information not listed as confidential or intended for internal use is public information. Information considered public in ADACOM is listed in section 2.2 of this CPS.

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

### **9.3.3 Responsibility to Protect Confidential Information**

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

Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information on the basis of a court order or in other cases provided by law.

## **9.4 *Privacy of Personal Information***

### **9.4.1 Privacy Plan**

ADACOM has implemented a privacy policy, which is located at:

<http://pki.adacom.com/repository> in compliance with the applicable laws.

#### **9.4.2 Information Treated as Private**

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

#### **9.4.3 Information Not Deemed Private**

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

#### **9.4.4 Responsibility to Protect Private Information**

ADACOM secures private information from compromise and disclosure to third parties and complies with all applicable privacy laws.

#### **9.4.5 Notice and Consent to Use Private Information**

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information are not used without the consent of the party to whom that information applies, in accordance with applicable privacy laws.

#### **9.4.6 Disclosure Pursuant to Judicial or Administrative Process**

ADACOM shall be entitled to disclose Confidential Information if, in good faith, ADACOM believes that:

- Disclosure is necessary in response to subpoenas and search warrants.
- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

#### **9.4.7 Disclosure upon Owner's Request**

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

#### **9.4.8 Other Information Disclosure Circumstances**

No stipulation.

### **9.5 *Intellectual Property rights***

The allocation of Intellectual Property Rights among ADACOM Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such ADACOM Sub-domain Participants. The following subsections apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

### **9.5.1 Property Rights in Certificates and Revocation Information**

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. ADACOM grants permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the General Terms and Conditions for Use of EU Qualified Certificates referenced in the Certificate. ADACOM grants permission to use revocation information to perform Relying Party functions subject to the applicable General Terms and Conditions for Use of EU Qualified Certificates, or any other applicable agreements.

### **9.5.2 Property Rights in the CPS**

Subscribers acknowledge that ADACOM retains all Intellectual Property Rights in and to this CPS.

### **9.5.3 Property Rights in Names**

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

### **9.5.4 Property Rights in Keys and Key Material**

Key pairs corresponding to Certificates of CAs and Subscribers are property of the CAs and Subscribers that are the respective Subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, Symantec's Root public keys and the Root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of Symantec. Symantec licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of those shares or the CA from Symantec or ADACOM.

## **9.6 Representations and Warranties**

### **9.6.1 CA Representations and Warranties**

ADACOM CA warrants that:

- Provides its services consistent with the requirements and the procedures defined in this CPS and related documents;
- Complies with eIDAS regulation and related legal acts defined in this CPS and related documents;
- Publishes its CPS and related documents and guarantees their availability in a public data communications network;
- Publishes and meet its claims in terms and conditions for subscribers and guarantees their availability and access in a public data communications network;
- Maintains confidentiality of the information which has come to its knowledge in the course of supplying the service and is not subject to publication;
- Keeps account of the Trust Service Tokens issued by it and their validity and ensure possibility to check the validity of certificates;
- Ensures the access to the private keys on the Remote QSCD to the authorized Subscriber of the keys
- Ensures the proper management and compliance of the Remote QSCD

- Informs the Supervisory Body of any changes to a public key used for the provision Trust Services;
- Without undue delay but in any event within 24 hours after having become aware of it, notify the Supervisory Body and, where applicable, other relevant bodies as national CERT or Data Inspectorate, of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein;
- Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach of security or loss of integrity without undue delay;
- Preserves all the documentation, records and logs related to Trust Services according to Sections 5.4 and 5.5;
- Ensures a conformity assessment according to requirements and present the conclusion of conformity assessment body to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- Has the financial stability and resources required to operate in conformity with this CPS;
- Publishes the terms of the compulsory insurance policy and the conclusion of conformity assessment body in a public data communications network;
- Does not restrict accessibility to its services for persons with disabilities.
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

ADACOM General Terms and Conditions for Use of EU Qualified Certificates may include additional representations and warranties.

### **9.6.2 RA Representations and Warranties**

ADACOM RA warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS and
- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects,

ADACOM General Terms and Conditions for Use of EU Qualified Certificates may include additional representations and warranties.

### **9.6.3 Subscriber Representations and Warranties**

Subscribers warrant that:

- Each EU Qualified e-Signature or e-Seal, created using the private key corresponding to the public key listed in the EU Qualified Certificate, is the EU Qualified e-Signature or e-Seal of the Subscriber and the EU Qualified Certificate has been accepted and is

operational (not expired or revoked) at the time the EU Qualified e-Signature or e-Seal is created,

- The credentials (PIN, PUK, username, password, OTP) accessing the private key are protected and that no unauthorized person has ever had access to them,
- ,
- EU Qualified e-Signature or e-Seal are only created by a QSCD device
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true, and the Subscriber is aware of the fact that ADACOM may refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;
- The Subscriber observes the requirements provided by ADACOM in this CPS and the related documents;
- All information supplied by the Subscriber and contained in the Certificate is true and in the event of a change in the data submitted, Subscriber shall notify the correct data in accordance with the rules established by this CPS and the related documents
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS
- The Subscriber is not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.
- The Subscriber shall notify ADACOM without any reasonable delay, if subject's private key or control to it has been lost, stolen, potentially compromised.

ADACOM General Terms and Conditions for Use of EU Qualified Certificates may include additional representations and warranties.

#### **9.6.4 Relying Party Representations and Warranties**

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

ADACOM General Terms and Conditions for Use of EU Qualified Certificates may include additional representations and warranties of Relying Parties.

#### **9.6.5 Representations and Warranties of Other Participants**

No stipulation.

#### **9.7 Disclaimers of Warranties**

To the extent permitted by applicable law, General Terms and Conditions for Use of Qualified Certificates disclaim ADACOM's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

ADACOM is not liable for:

- The secrecy of the credentials (PIN, PUK, username, password, OTP) that have access to the private keys of the Subscribers, possible misuse of the certificates or inadequate checks of the certificates or for the wrong decisions of a Relying Party or any consequences due to errors or omission in Trust Service validation checks;

- The non-performance of its obligations if such non-performance is due to faults or security problems of the Supervisory Body, the data protection supervision authority, Trusted List or any other public authority;
- Non-fulfilment of the obligations arising from this CPS and the related documents if such non-fulfilment is occasioned by Force Majeure.

## **9.8 Limitations of Liability**

ADACOM General Terms and Conditions for Use of EU Qualified Certificates limit ADACOM's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the liability cap of five hundred Euros (500.00 €) limiting ADACOM's damages concerning an EU Qualified Certificate.

The liability (and/or limitation thereof) of Subscribers and Relying Parties is as set forth in the applicable General Terms and Conditions for Use of EU Qualified Certificates.

## **9.9 Indemnities**

### **9.9.1 Indemnification by Subscribers**

To the extent permitted by applicable law, Subscribers are required to indemnify ADACOM for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The General Terms and Conditions for Use of EU Qualified Certificates may include additional indemnity obligations.

### **9.9.2 Indemnification by Relying Parties**

To the extent permitted by applicable law, ADACOM General Terms and Conditions for Use of EU Qualified Certificates requires Relying Parties to indemnify ADACOM for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The General Terms and Conditions for Use of EU Qualified Certificates may include additional indemnity obligations.

## **9.10 Term and Termination**

### **9.10.1 Term**

The CPS becomes effective upon publication in the ADACOM repository. Amendments to this CPS become effective upon publication in the ADACOM repository.



### **9.10.2 Termination**

This CPS as amended from time to time remains in force until it is replaced by a new version.

### **9.10.3 Effect of Termination and Survival**

Upon termination of this CPS, ADACOM Sub-domain Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

## **9.11 *Individual Notices and Communications with Participants***

Unless otherwise specified by agreement between the parties, ADACOM Sub-domain Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

## **9.12 *Amendments***

### **9.12.1 Procedure for Amendment**

Amendments to this CPS are made by the ADACOM Policy Management Authority (PMA). Amendments are either in the form of a document containing an amended form of the CPS or an update. Amended versions or updates are linked to ADACOM Repository located at: <https://pki.adacom.com/repository>. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies.

### **9.12.2 Notification Mechanism and Period**

ADACOM's PMA reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion.

Proposed amendments to the CPS are linked to ADACOM Repository located at: <https://pki.adacom.com/repository>.

Notwithstanding anything in the CPS to the contrary, if the PMA believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the TSP or any portion of it, ADACOM and the PMA shall be is entitled to make such amendments by publication in the ADACOM Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, ADACOM provides notice to of such amendments to ADACOM Sub-domain Participants.

At a minimum ADACOM and the PMA will update this CPS annually in compliance with CA/Browser Forum guidelines.

Amendments which do not change the meaning of this CPS, such as spelling corrections, translation activities and contact details updates are documented in the Versions and Changes section of the present document. In this case the fractional part of the document version number is enlarged.

In case of substantial changes, the new CPS version is clearly distinguishable from the previous ones and the serial number is enlarged by one.

### **9.12.3 Circumstances under Which OID Must be changed**

If the PMA, in cooperation with Symantec, determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment contains new object identifiers for the Certificate policies. Otherwise, amendments shall not require a change in Certificate policy object identifier.

## ***9.13 Dispute Resolution Provisions***

### **9.13.1 Disputes among Symantec, Affiliates, and Customers**

Disputes among ADACOM Sub-domain Participants are resolved pursuant to provisions in the applicable agreements among the parties.

### **9.13.2 Disputes with Subscribers or Relying Parties**

ADACOM General Terms and Conditions for Use of EU Qualified Certificates contain a dispute resolution clause. Disputes involving ADACOM require an initial negotiation period of sixty (60) days followed by litigation in the courts of Athens- Greece.

## ***9.14 Governing Law***

The law of Greece governs the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Greece. This choice of law is made to ensure uniform procedures and interpretation for all ADACOM Sub-domain Participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

## ***9.15 Compliance with Applicable Law***

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:
  - a. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
  - b. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
  - c. 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;

- CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates

## **9.16 *Miscellaneous Provisions***

### **9.16.1 Entire Agreement**

Not applicable.

### **9.16.2 Assignment**

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of ADACOM. Unless specified otherwise in a contract with a party, ADACOM does not provide notice of assignment.

### **9.16.3 Severability**

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

### **9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)**

ADACOM may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. ADACOM's failure to enforce a provision of this CPS does not waive ADACOM's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by ADACOM

### **9.16.5 Force Majeure**

Non-fulfilment of the obligations arising from the CPS and/or related documents is not considered a violation if such non-fulfilment is occasioned by Force Majeure. None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this CPS and/or related documents caused by Force Majeure.

## **9.17 *Other Provisions***

Not applicable.

## Appendix A. Table of Acronyms and definitions

### Table of Acronyms

Term	Definition
<b>CA</b>	Certification Authority.
<b>CP</b>	Certificate Policy.
<b>CPS</b>	Certification Practice Statement.
<b>CRL</b>	Certificate Revocation List.
<b>CSR</b>	Certificate Signing Request
<b>FIPS</b>	United State Federal Information Processing Standards.
<b>LRA</b>	Local Registration Authority
<b>NCP</b>	Normalized Certificate Policy
<b>NCP+</b>	Extended Normalized Certificate Policy
<b>OCSP</b>	Online Certificate Status Protocol.
<b>OID</b>	Object Identifier, a unique object identification code
<b>PCA</b>	Primary Certification Authority.
<b>PDS</b>	PKI Disclosure Statement
<b>PIN</b>	Personal identification number.
<b>PKCS</b>	Public-Key Cryptography Standard.
<b>PKI</b>	Public Key Infrastructure.
<b>PMA</b>	Policy Management Authority.
<b>QSCD</b>	Qualified Electronic Signature Creation Device
<b>RA</b>	Registration Authority.
<b>RFC</b>	Request for comment.
<b>SSL</b>	Secure Sockets Layer.
<b>STN</b>	Symantec Trust Network.
<b>TSP</b>	Trust Service Provider

### Definitions

Term	Definition
<b>ADACOM Repository</b>	ADACOM's database of Certificates and other relevant ADACOM information accessible on-line.
<b>Administrator</b>	A Trusted Person within the organization that performs validation and other CA or RA functions.
<b>Administrator Certificate</b>	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
<b>Advanced electronic seal</b>	An electronic seal that meets the following requirements: <ul style="list-style-type: none"> <li>• it is uniquely linked to the creator of the seal;</li> <li>• it is capable of identifying the creator of the seal;</li> <li>• it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and</li> <li>• it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.</li> </ul>
<b>Advanced electronic signature</b>	An electronic signature that meets the following requirements <ul style="list-style-type: none"> <li>• it is uniquely linked to the signatory;</li> <li>• it is capable of identifying the signatory;</li> <li>• it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and</li> </ul>

<b>Term</b>	<b>Definition</b>
	<ul style="list-style-type: none"> <li>it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.</li> </ul>
<b>Certificate</b>	Public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it
<b>Certificate Applicant</b>	An individual or organization that requests the issuance of a Certificate by a CA.
<b>Certificate Application</b>	A request from a Certificate to a CA for the issuance of a Certificate.
<b>Certificate Chain</b>	An ordered list of Certificates containing a Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
<b>Certificate Policy (CP)</b>	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
<b>Certificate Revocation List (CRL)</b>	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer
<b>Certificate Signing Request (CSR)</b>	A message conveying a request to have a Certificate issued.
<b>Certification Authority (CA)</b>	An entity authorized to create and assign certificates
<b>Certification Practice Statement (CPS)</b>	Statement of the practices which a Certification Authority employs in issuing, managing, revoking, and renewing or re-keying certificates
<b>Challenge Phrase</b>	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke the Subscriber's Certificate.
<b>Compliance Audit</b>	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.
<b>Compromise</b>	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.
<b>eIDAS</b>	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.
<b>Electronic Signature</b>	Data in electronic form which are attached to or logically associated with other electronic data and which is used by the signatory to sign.
<b>Electronic seal</b>	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
<b>Exigent Audit/Investigation</b>	An audit or investigation by Symantec or ADACOM where ADACOM has reason to believe that an entity failed to meet STN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the STN posed by the entity has occurred.
<b>Intellectual Property Rights</b>	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
<b>Intermediate Certification Authority (Intermediate CA)</b>	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
<b>Key Generation Ceremony</b>	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
<b>Local QSCD</b>	USB token or smart card of QSCD
<b>Long-lived Certificate</b>	A Qualified Certificate which is valid for 1 to 3 years.
<b>Manual Authentication</b>	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.

<b>Term</b>	<b>Definition</b>
<b>Non-repudiation</b>	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a STN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
<b>Offline CA</b>	Symantec PCAs Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
<b>Online CA</b>	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
<b>Online Certificate Status Protocol (OCSP)</b>	A protocol for providing Relying Parties with real-time Certificate status information.
<b>OTP</b>	One Time Password
<b>Operational Period</b>	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.
<b>PKCS #10</b>	Public-Key Cryptography Standard #10 developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
<b>PKCS #12</b>	Public-Key Cryptography Standard #12 developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
<b>Policy Management Authority (PMA)</b>	The organization within ADACOM responsible for promulgating this policy.
<b>Practice Statement</b>	A statement of the practices that a TSP employs in providing a Trust Service.
<b>Private key</b>	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create a qualified certificate or to decrypt electronic records or files that were encrypted with the corresponding public key
<b>Primary Certification Authority (PCA)</b>	A CA that acts as a root CA and issues Certificates to CAs subordinate to it.
<b>Processing Center</b>	The ADACOM site that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates.
<b>Public Key</b>	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.
<b>Public Key Infrastructure (PKI)</b>	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.
<b>Qualified electronic seal</b>	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.
<b>Qualified electronic Signature</b>	An advanced electronic signature that is created by a qualified electronic signature creation device, and is based on a qualified certificate for electronic signatures;
<b>Qualified Certificate</b>	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.
<b>Qualified signature creation device (QSCD)</b>	A device that is responsible for qualifying digital signatures by using specific hardware and software that ensures that the signatory only has control of their private key. Qualified electronic signature or seal creation devices meet the requirements of eIDAS.

<b>Term</b>	<b>Definition</b>
<b>Qualified Trust Service Provider</b>	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body.
<b>Registration Authority (RA)</b>	An entity approved by a CA that is responsible for identification and authentication of subjects of certificates. Additionally an RA can assist in the certificate application process or revocation process or both.
<b>Relying Party</b>	An individual or organization that acts in reliance on a certificate.
<b>Remote QSCD</b>	Server based HSM that is used for central generation and usage of Subscriber private keys.
<b>Remote ID verification</b>	The method/process by which the Subscriber is identified through a live video call session and is equivalent to validation through physical presence.
<b>Root CA</b>	Certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s).
<b>RSA</b>	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
<b>Secret Share</b>	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
<b>Secret Sharing</b>	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations
<b>Secure Sockets Layer (SSL)</b>	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
<b>Security and Audit Requirements Guide</b>	A Symantec document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
<b>Short-lived Certificate</b>	A Qualified Certificate which is valid from 24 to 72 hours and can be used for one transaction.
<b>Sub-domain</b>	The portion of the STN under control of an entity and all entities subordinate to it within the STN hierarchy.
<b>Subordinate CA</b>	Certification authority who's 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.
<b>Subject</b>	The subject can be: a) a natural person; b) a natural person identified in association with a legal person; c) a legal person (that can be an Organization or a unit or a department identified in association with an Organization);
<b>Subscriber</b>	An entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations.
<b>Supervisory Body</b>	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.
<b>Symantec</b>	Means, with respect to each pertinent portion of this CPS, Symantec Corporation and/or any wholly owned Symantec subsidiary responsible for the specific operations at issue.
<b>Trust Service</b>	Electronic service for: <ul style="list-style-type: none"> <li>• creation, verification, and validation of digital signatures and related certificates;</li> <li>• creation, verification, and validation of time-stamps and related certificates;</li> <li>• registered delivery and related certificates;</li> <li>• creation, verification and validation of certificates for website authentication; or</li> <li>• preservation of digital signatures or certificates related to those services.</li> </ul>
<b>Trust Service Provider</b>	An entity that provides one or more Trust Services.
<b>Trusted Person</b>	An employee, contractor, or consultant of an entity, responsible for managing



<b>Term</b>	<b>Definition</b>
	infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
<b>Trusted Position</b>	The positions within ADACOM that must be held by a Trusted Person.
<b>Trustworthy System</b>	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.
<b>Symantec Trust Network (STN)</b>	The Certificate-based Public Key Infrastructure governed by the Symantec Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by Symantec and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
<b>STN Participant</b>	An individual or organization that is one or more of the following within the STN: Symantec, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
<b>STN Standards</b>	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the STN.
<b>General Terms and Conditions for Use of Qualified Certificates</b>	A binding document setting forth the terms and conditions under which an a natural or legal person acts as a Subscriber or as a Relying Party and ADACOM provides the corresponding Trust Services.
<b>Valid Certificate</b>	A Certificate that passes the validation procedure specified in RFC 5280.
<b>Validity Period</b>	The period of time measured from the date when the Certificate is issued until the Expiry Date.