ADACOM Certification Practice Statement for non-Qualified Certificates

Version 4.1

Effective Date: 15.07.2020

ADACOM S.A.
25 Kreontos Street
10442 Athens
Greece
Phone number: +30 210 5193 740
https://www.adacom.com

ADACOM Certification Practices Statement for Non-Qualified certificates

Trademark Notices

Version History		
Date	Version	Changes
31.05.2009	3.0	Initial document
31.05.2010	3.5.0	Minor changes
30.09.2010	3.7.0	Minor changes
01.01.2011	3.8.0	Minor changes
01.04.2011	3.8.1	Minor changes
01.12.2011	3.8.2	Minor changes
01.06.2012	3.8.3	Minor changes
25.05.2015	3.8.4	Minor changes
01.04.2020	4.0	Major changes to align with DigiCert CP
15.07.2020	4.1	Minor changes in paragraphs 1.1, 1.4.1, 1.2, 3.1.2, 3.2.3, 3.2.6, 4.9.1, 4.9.2, 5.5.2, 6.2.8, 7.1.6

Table of Contents

1. INTRODUCTION

This document is the ADACOM Certification Practice Statement ("CPS") for Non-Qualified Certificates ("Certificates"). It states the practices that ADACOM as a Trusted Service Provider (TSP) employs in providing certification services for Certificates in accordance but not limited to the specific requirements of the DigiCert Certificate Policy ("CP") regarding Primary Certification Authorities.

The CP is the principal statement of policy which defines the procedural and operational requirements that DigiCert requires entities to adhere to when issuing and managing digitally signed objects within DigiCert's PKI. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the DigiCert PKI and providing associated trust services. These requirements apply to all Certificate Authorities (CAs), Registration Authorities (RAs), Processing Centers, Affiliates, Subscribers, Relying Parties, and other PKI entities that interoperate with or within the DigiCert PKI, and thereby provide assurances of uniform trust throughout DigiCert's PKI. More information concerning the DigiCert PKI is available in the DigiCert CP.[1]

ADACOM has authority over a portion of the DigiCert PKI called its "Sub CA" of the DigiCert PKI. ADACOM's PKI includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CPs set forth requirements that ADACOM must meet, this CPS describes how ADACOM meets these requirements and describes the practices that ADACOM employs for:

- Securely managing the related infrastructure that supports the DigiCert PKI, and
- Issuing, maintenance and life-cycle management of Certificates

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 for issuing, maintenance and lifecycle management of Certificates.

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 within DigiCert's PKI and performs all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates.

ADACOM offers the following types of non-qualified certificates within its Sub-domain of the DigiCert PKI:

- Class 1
- Class 2 (for the Managed PKI users)

This CPS is specifically applicable to:

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

[1] The current version of DigiCert CP can be found at https://pki.adacom.com/repository

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[3] 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.
- Ancillary agreements impose by ADACOM. These agreements bind Customers, Subscribers and Relying parties. Among other things, these agreements state specific practices for how DigiCert's PKI Policies must be followed.

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

1.2 Document name and Identification

This document is the ADACOM Certification Practice Statement for non-Qualified Certificates. Certificates contain object identifier values corresponding to the applicable Class of Certificate. Therefore, ADACOM has not assigned this CPS an object identifier value. Certificate Policy Object Identifiers are used in accordance with Section 7.1.6.

ADACOM Certificates are issued according to the following certificate policies:

OID 2.16.840.1.113733.1.7.23.1 joint-iso-itut(2) country(16) us(840) organization(1) symantec(113733) pki(1) policies(7) vtn-cp(23) class1(1)	**Maps to OID** 2.16.840.1.114412.4.1.1 or 2.16.840.1.114412.5.1
OID 2.16.840.1.113733.1.7.23.2 joint-iso-itut(2) country(16) us(840) organization(1) symantec(113733) pki(1) policies(7) vtn-cp(23) class2(2)	**Maps to OID** 2.16.840.1.114412.4.2 or 2.16.840.1.114412.5.2

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the DigiCert PKI. The CA term encompasses a subcategory of

[3] Although these documents are not publicly available they may be made available to customer under special agreement.

issuers called Primary Certification Authorities (PCA). PCAs act as roots of four domains[4], one for each class of Certificate. Each PCA is a DigiCert entity. Subordinate to the PCAs are ADACOM Certification Authorities that issue Certificates to end-user Subscribers or other CAs.

ADACOM enterprise customers may operate their own CAs as a subordinate CA to a DigiCert PCA. Such a customer enters into a contractual relationship with ADACOM to abide by all the requirements of the DigiCert CP and the ADACOM CPS. These subordinate CAs may, however implement more restrictive practices based on their internal requirements.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a DigiCert CA. ADACOM acts as an RA for the end user certificates it issues.

Third parties, who enter into a contractual relationship with ADACOM, may operate their own RA and authorize the issuance of certificates by an ADACOM CA. Third party RAs must abide by all the requirements of the DigiCert CP, the ADACOM CPS and the terms of their enterprise services agreement with ADACOM. RAs may, however implement more restrictive practices based on their internal requirements.

ADACOM may 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, and the terms of the LRA Agreement signed between LRA and ADACOM.

ADACOM may also enter into a contractual relationship with one or more third parties, in order to outsource all RA responsibilities. In this case, the third party becomes a RA and performs its responsibilities in full compliance with this CPS, and the terms of the RA Agreement signed between RA and ADACOM

Validation of domain portion of the email address cannot be delegated to a third party and is only validated by the RA of the Issuer CA.

1.3.3 Subscribers

Subscribers under the DigiCert PKI include all end users (including entities) of certificates issued by a DigiCert CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals or organizations.

In some cases, certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). 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.

When 'Subject' is used, it is to indicate a distinction from the Subscriber. When "Subscriber" is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within the DigiCert PKI, either as a PCA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CPS, however, apply only to end-user Subscribers.

1.3.4 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 DigiCert PKI. A Relying party may, or may not also be a Subscriber within the DigiCert PKI.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While the most common usages for individual certificates are included in the table below, an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, the DigiCert CP, the CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	**Assurance Level**			**Usage**		
	Low assurance level	**Medium assurance Level**	**High assurance Level**	**Signing**	**Encryption**	**Client Authentication**
Class 1 Certificates	✓			✓	✓	✓
Class 2 Certificates		✓		✓	✓	✓

1.4.1.1 Assurance levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.
Medium assurance certificates are certificates that are suitable for securing some inter and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity, in relation to Class 1 and 3.
High assurance Certificates are individual certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and Class 2 Certificates.

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.

DigiCert and ADACOM Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, Class 1 Certificates shall not be used as proof of identity or as support of non-repudiation of identity or authority. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

DigiCert 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 should 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

Attn: ADACOM Policy Management Authority
Telephone number: +30 210 5193740
fax number: +30 210 5193555
email: practices@adacom.com

1.5.2 Contact Person

ADACOM Policy Management Authority
25, Kreontos Street,10442, Athens Greece

Telephone number +30 210 5193740
fax number: +30 210 5193555 email:
practices@adacom.com

1.5.3 Person Determining CP Suitability for the Policy

The organization identified in Section 1.5.2 is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the DigiCert CP and this CPS.

1.5.4 CPS Approval Procedure

Approval of this CPS and subsequent amendments 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 notice. Amended versions or updates shall be published at http://pki.adacom.com/repository.
Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

1.7 References

Name of Policy/Guideline/Requirement Standard	**Location of Source Document**
DigiCert Certificate Policy version 5.0	https://pki.adacom.com/repository
DigiCert Certification Practices Statement version 5.0	https://www.digicert.com/legal-repository/
The Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	https://cabforum.org/baseline-requirements-document/

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ADACOM is responsible for the repository functions for its own CAs and the CAs of its Enterprise Customers. The Certificates that ADACOM issues, are published in the repository in accordance with CPS Section 2.2.

Upon revocation of an end-user Subscriber's Certificate, ADACOM publishes notice of such revocation in the repository. ADACOM issues Certificate Revocation Lists (CRLs) for its own CAs and the CAs of Service Centers and Enterprise Customers within its Sub-domain, pursuant to the provisions of this CPS. In addition, for the Enterprise Customers who have contracted for Online Certificate Status Protocol ("OCSP") services, ADACOM provides OCSP services pursuant to the provisions of this CPS.

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
- 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

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

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

Unless where indicated otherwise in the DigiCert CP, this CPS or the content of the digital certificate, names appearing in Certificates issued under DigiCert PKI are authenticated.

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 published 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

Class 2 Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual 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

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

ADACOM ensures that Subject Distinguished Names of a Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name.

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-approved and DigiCert-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organization identity

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in ADACOM's documented Validation Procedures.

At a minimum ADACOM:

- Determines that the organization 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 agency or competent authority that confirms the existence of the organization,
- Confirms by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization is also confirmed.

Where an e-mail address is included in the certificate, ADACOM authenticates the Organization's right to use that e-mail domain.

3.2.3 Authentication of Individual Identity

Authentication of individual identity differs according to the Class of Certificate. The minimum authentication standard for each class of certificate is explained in the table below.

Certificate Class	Authentication of Identity
Class 1	No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.
Class 2	Authenticate identity by matching the identity provided by the Subscriber to: • information residing in the database of a ADACOM - approved identity proofing service, or • 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.

3.2.4 Domain Email validation

ADACOM verifies a Subscriber's right to use or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by sending an approval email message to the email address to be included in the Certificate and by sending a unique Random Value by SMS to the mobile number provided in the signed application form by the Subscriber.

3.2.5 Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU),
- Subscriber's name in Class 1 certificates,
- Any other information designated as non-verified in the certificate.

3.2.6 Validation of Authority

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

- determines that the organization 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 organization, 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 organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

3.2.7 Criteria for Interoperation

ADACOM may provide interoperation services that allow a non-DigiCert CA to be able to interoperate with the DigiCert PKI by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with the DigiCert CP as supplemented by additional policies when required.

ADACOM only allows interoperation with the DigiCert PKI of a non-DigiCert CA in circumstances

where the CA, at a minimum:

- Enters into a contractual agreement with ADACOM,
- Operates under a CPS that meets DigiCert requirements for the classes of certificates it will issue,
- Passes a compliance assessment before being allowed to interoperate,
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's 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") However, in certain cases Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes and Types of ADACOM Certificates this distinction is not important as a new key pair is always generated as part of ADACOM's end-user Subscriber Certificate replacement process.

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

The Subscriber submits a rekey application to ADACOM or the equivalent RA by submitting his existing certificate (digitally signing), and ADACOM or the RA, reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application, as described in section 3.2.3.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key after revocation is not permitted if the revocation occurred because:

- the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or

- the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person or entity named as the Subject of such Certificate, or
- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.
- For any other reason deemed necessary by DigiCert or ADACOM to protect the DigiCert PKI.

Subject to the foregoing paragraph, renewal of CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate.

Renewal of a Certificate following revocation must ensure that the person seeking renewal is, in fact, the Subscriber. The requirements for the identification and authentication of an original Certificate Application are used for renewing a Certificate following revocation.

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, or the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include one or more of the following, depending on the certificate Class:

- 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 digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate, ensuring that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

ADACOM Administrators are entitled to request the revocation of end-user Subscriber Certificates within ADACOM's Sub-domain. ADACOM authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another DigiCert-approved procedure.

RAs using an Automated Administration Software Module may submit bulk revocation requests to ADACOM. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

The requests to revoke a CA Certificate are authenticated by the ADACOM to ensure that the revocation has in fact been requested by the CA.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of a CA,
- Any authorized representative of an RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-user Certificate Subscribers

All end-user Certificate Subscribers manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to ADACOM
- demonstrating possession of the private key corresponding to the public key delivered to ADACOM.

4.1.2.2 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with ADACOM. CA and RA Applicants provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant cooperates with ADACOM to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

ADACOM or an RA perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

ADACOM or an RA 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 or an RA 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
- The Subscriber fails to respond to notices within a specified time, or

- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring DigiCert into disrepute.

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 Subscriber Agreement, CPS or other Agreement between DigiCert PKI participants.
A certificate application remains active until rejected.

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 or following receipt of an RA's request to issue the Certificate. ADACOM creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

ADACOM either directly or through an RA, 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 end-user Subscribers, by informing them to download them from a web site via an email message sent to the Subscriber.

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 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 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 Subscriber agreement and accepted the certificate. The certificate shall be used lawfully in accordance with ADACOM's Subscriber Agreement.

CP and this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable relying party agreement 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 (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- 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 digital 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

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. ADACOM does not support this service.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

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. Certificate rekey is supported for all certificate Classes.

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 for an individual certificate may request certificate rekeying.

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information) has not changed, a renewal Certificate is automatically issued. Subject to the provisions of Section 3.3.1, after re-keying in this fashion, and on at least alternative instances of subsequent re-keying thereafter, ADACOM or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

The Subscriber submits a rekey application to ADACOM or the equivalent RA by submitting his existing certificate (digitally signing), and ADACOM or the RA, reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application, as described in section 3.2.3.

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 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 or an RA shall perform 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

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, all revocation requests are authenticated.

Revocation of certificates is performed according to the following sections.

For certificates including email address, certificate revocation and suspension is compliant with CA/B Forum Requirements

4.9.1 Circumstances for Revocation

The ADACOM Subscriber's agreement provides the obligation or/and right to the parties to request revocation of a Certificate. Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by ADACOM (or by the Subscriber) and published on a CRL. Upon request from a subscriber who can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, ADACOM will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:

- ADACOM, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- ADACOM or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- ADACOM or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the Subject of such Certificate,
- ADACOM or a Customer has reason to believe that a material fact in the Certificate Application is false,
- ADACOM or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed, or
- A final court judgment requires the relevant revocation or cancellation
- If the private key of the CA has been compromised.
- The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has been changed, or when the Subscriber uses the Certificate in a specific capacity, loses the said capacity (indicatively, in case of retirement of an employee to whom such a certificate has been issued in his/her capacity as an employee serving for a certain agency or in a certain position) or in any case where any data included in the certificate are altered,
- The Subscriber identity has not been successfully re-verified in accordance with section 6.3.2,
- The Subscriber has not submitted payment when due, or
- The continued use of that certificate is harmful to DigiCert.
- For Certificates including an email address) they no longer comply with the requirements of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy.

When considering whether certificate usage is harmful to DigiCert, 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 Subscriber Agreements require end-user 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

Individual Subscribers or a duly authorized person by them can request the revocation of their own individual Certificates through an authorized representative of ADACOM. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

ADACOM is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to ADACOM by e-mail at customer-support@adacom.com or by telephone at +30 210 9577255 or to the Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly. For Enterprise customers, the Subscriber is required to communicate the request to the Enterprise Administrator who will communicate the revocation request to ADACOM for processing. Communication of such revocation request shall be in accordance with CPS § 3.4.

Where an Enterprise Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer instructs ADACOM to revoke the Certificate.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to ADACOM. ADACOM will then revoke the Certificate. ADACOM may also initiate CA or RA Certificate revocation.

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.

Right after the approval of a revocation request, the CA informs 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 either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

4.9.7 CRL Issuance Frequency

CRLs for end-user 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. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

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, where offered, OCSP. In addition to publishing CRLs, ADACOM provides Certificate status information through query functions in the ADACOM repository.

Certificate status information is available through web-based query functions accessible through the ADACOM Repository at

- https://onsite.adacom.com/services/ADACOMSAConsumerServiceCenterClass1/client/search.htm for Class 1, and
- https://onsite.adacom.com/services/ADACOMSAConsumerServiceCenterClass2/client/search.htm for Class 2

ADACOM also provides OCSP Certificate status information. Enterprise Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Enterprise Customer.

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 applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

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 their own CAs or one of the CAs within their sub-domains.

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 at ADACOM's website, LDAP directory and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services are available 24◂7 without scheduled interruption.

4.10.3 Optional Features

OCSP is an optional status service feature that is not available for all products and must be specifically enabled for other products.

4.11 End of Subscription

A subscriber may end a subscription for an ADACOM certificate by:

- Allowing his/her/its certificate to expire without renewing or re-keying that certificate,
- Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

With the exception of enterprises deploying Managed PKI Key Management Services no DigiCert PKI participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using Managed PKI Key Management Service (KMS) can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. The enterprise customer may use KMS operated either out of the enterprise's premises or ADACOM's secure data center. If operated out of the enterprise's premises, ADACOM does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

Enterprise customers using the Managed PKI Key Management service (or an equivalent service approved by ADACOM) are permitted to escrow end-user Subscribers' private key. Escrowed private keys are stored in encrypted form using the Managed PKI Key Manager software. Except for enterprise customers using the Managed PKI Key Manager Service (or an equivalent service approved by ADACOM), the private keys of CAs or end-user Subscribers are not escrowed.

End-user Subscriber private keys are only recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator's Guide, under which:

- Enterprise customers using Managed PKI Key Manager confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an imposter,
- Enterprise customers recover a Subscriber's private key without the Subscriber's authority only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose
- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

It is recommended that Enterprise Customers using KMS:

- Notify the subscribers that their private keys are escrowed
- To explicitly inform, via the applicable Subscriber and Relying Party Agreements the end user and the Relying Parties respectively, that the end user is not supposed to use the encryption key pair for signing purposes.
- Protect subscribers' escrowed keys from unauthorized disclosure,
- Protect all information, including the administrator's own key(s) that could be used to recover subscribers' escrowed keys.
- Release subscribers' escrowed keys only for properly authenticated and authorized requests for recovery.
- Revoke the Subscriber's Key pair prior to recovering the encryption key under certain circumstances such as to discontinue the use of a lost certificate.
- Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery.
- Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organization policy; or by order of a court of competent jurisdiction.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored in the Key Manager database in encrypted form. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key. A Key Escrow Record (KER)

is generated, then the triple-DES key is combined with a random session key to form a session key mask. The resulting masked session key (MSK) is securely sent and stored in the Managed PKI database at ADACOM. The KER (containing the end user's private key) and the random session key mask are stored in the Key Manager database and all residual key material is destroyed.

The Managed PKI database is operated out of ADACOM's secure data center. The enterprise customer may choose to operate the Key Manager database either on the enterprise's premises or out of ADACOM's secure data center.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the "recover" link is the MSK for that key pair returned from the Managed PKI database. The Key Manager retrieves the session key from the KMD and combines it with the MSK to regenerate the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

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. The 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 comply with the Off-site Storage Security Requirements set forth in the "ADACOM Disaster Recovery Plan for the Interim Offsite Storage of Cryptographic Materials" and the "ADACOM Disaster Recovery Plan".

5.1.2 Physical Access

ADACOM CA systems are protected by seven 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.

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 and 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, and electromagnetic).

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 a secure off-site storage 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, renewal 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,
- 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.

Independent contractors and consultants that have access to or control authentication or cryptographic operations, are allowed to conduct these operations only to the extent they are escorted and directly supervised by Trusted Persons at all times.

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.

Other manual operations not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing ADACOM HR or security functions and a check of well-recognized forms of identification (e.g., passports and identification cards). Identity is further confirmed through the background checking procedures in CPS § 5.3.1.

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.

5.2.4 Roles Requiring Separation of Duties

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

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, recovery requests or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests;
- the generation, issuing or destruction of a CA certificate;
- the loading of a CA on production.

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 competently and satisfactorily.

5.3.2 Background Check Procedures

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

- 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

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken 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 CPS § 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 manually or automatically logs the following significant events:

- CA key life cycle management events, including:
    - Key generation, backup, storage, recovery, archival, and destruction

    - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
    - Certificate Applications, renewal, rekey, and revocation
    - Successful or unsuccessful processing of requests
    - Generation and issuance of Certificates and CRLs.
- Security-related events including:
    - Successful and unsuccessful PKI system access attempts
    - PKI and security system actions performed by ADACOM personnel
    - Security sensitive files or records read, written or deleted
    - Security profile changes
    - System crashes, hardware failures and other anomalies
    - Firewall and router activity
    - CA facility visitor 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 RAs and Enterprise Administrators 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 drivers license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

5.4.2 Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, ADACOM reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within ADACOM CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities 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 onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

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.

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.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity's annual Compliance 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 e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked.

- Five (5) years for Class 1 Certificates,
- Ten (10) years and six (6) months for Class 2 Certificates.

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 of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained using an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

ADACOM archive collection systems are internal, except for enterprise RA Customers. ADACOM assists its enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA.

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.

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 will be 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 CP § 6.2.4. ADACOM maintains backups of the foregoing CA information for their own CAs, as well as the CAs of Enterprise Customers within its Sub-domain.

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 a ADACOM CA, ADACOM infrastructure or Customer CA private key, ADACOM's Key Compromise Response procedures are enacted by the ADACOM Security Incident Response Team (ASIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other ADACOM management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from ADACOM executive management.

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 CPS § 4.4.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected DigiCert PKI Participants, and
- The CA will generate a new key pair in accordance with CPS § 4.7, except where the CA is being terminated in accordance with CPS § 4.9.

5.7.4 Business Continuity Capabilities After a Disaster

ADACOM has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. ADACOM's disaster recovery site has implemented the physical security protections and operational controls required by the ADACOM Information Security Management System (ISMS) to provide for a secure and sound backup operational setup.
In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from ADACOM's primary facility, ADACOM's disaster recovery process is initiated by the ADACOM team in charge.

ADACOM has the capability to restore or recover operations with top priority with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- publication of revocation information, and
- provision of key recovery information for Enterprise Customers using Managed PKI Key Manager.

ADACOM's disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.1.

ADACOM's disaster recovery plan has been designed to provide full recovery following disaster occurring at ADACOM's primary site. ADACOM tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Where possible, operations are resumed at ADACOM's primary site as soon as possible following a major disaster.

ADACOM maintains backups of its CA and infrastructure system software at a secure offsite location. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4. Specifically, they are backed up, in accordance with "ADACOM Disaster Recovery Plan for the Interim Offsite Storage of Cryptographic Materials", which will allow for business resumption at a later date.

ADACOM also maintains offsite backups of important CA information for ADACOM CAs as well as

the CAs of Enterprise Customers, within ADACOM's Sub-domain. Such information includes, but is not limited to: Certificate Application data, audit data (per CPS § 4.5), and database records for all Certificates issued.

5.8 CA or RA Termination

In the event that it is necessary for an ADACOM CA, or Enterprise Customer 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", and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans 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 and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.
- Provision of notice to the Greek Supervisory Authority.

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. For PCA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of CC EAL 4+ and FIPS 140-1 level 3. For other CAs (including ADACOM CAs and Enterprise Customer CAs), the cryptographic modules used meet the requirements of at least CC EAL 4+ and FIPS 140-1 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 and the CA Key Management Tool User's 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 RA key pairs is generally performed by the RA using a CC EAL 4+ and FIPS 140-1 level 1 certified cryptographic module provided with their browser software.

Enterprise Customers generate the key pair used by their Automated Administration servers. ADACOM recommends that Automated Administration server key pair generation be performed using a CC EAL 4+ and FIPS 140-1 level 2 certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. For Class 1 and Class 2 Certificates, the Subscriber typically uses a CC EAL 4+ and FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation.

6.1.2 Private Key Delivery to Subscriber

End-user Subscriber key pairs are generated by the end-user Subscriber, thus private key delivery to a Subscriber is not applicable.

Where end-user Subscriber key pairs are pre-generated by ADACOM or Enterprise Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Enterprise Customer.

For Enterprise Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of Subscribers whose Certificate Applications they approve) and transmit such key pairs to Subscribers via a password protected PKCS # 12 file.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs 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 CA, key pairs are generated by ADACOM, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

ADACOM makes the CA Certificates for DigiCert PCAs and its root CAs available to Subscribers and Relying Parties through their inclusion in web browser software. As new PCA and root CA Certificates are generated, ADACOM 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 end-user 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. This is a process controlled by the PKI application. 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 at http://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.
Currently, ADACOM generates and uses at least the following minimum key sizes, signature algorithms, and hash algorithms for signing Certificates, CRLs, and certificate status server responses:

- RSA keys whose modulus size in bits is divisible by 8, and is at least 2048;
- Digest algorithms: SHA-256, SHA-384, or SHA-512.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

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 and Enterprise Customer CA private keys. Subscribers are required by contract 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 PCA and Issuing Root CA key pair generation and CA private key storage, ADACOM uses hardware cryptographic modules that are certified at or meet the requirements of CC EAL 4+ and FIPS 140-1 Level 3. For the rest ADACOM CAs, hardware cryptographic modules that are certified at or meet the requirements stated in section § 6.1.1 of this CPS.

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 3. The number of shares distributed for disaster recovery tokens it's the same as the number distributed for operational tokens, and the threshold number of required shares remains the same, as well. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

ADACOM CA and end user's private keys are not escrowed. Enterprise Customer may choose either to escrow or not its end user private keys. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private Key Backup

ADACOM creates backup copies of CA private keys 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 CA private key storage meet the requirements of this CPS. CA 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.

ADACOM does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12.

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, unless the CA Certificate has been renewed in terms of this CPS.

ADACOM does not archive copies of RA and Subscriber private keys.

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.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Key

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

6.2.8.1 Class 1 Certificates

The Standard for Class 1 private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, ADACOM recommends that Subscribers use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Class 2 Certificates

The Standard for Class 2 Private Key protection is for Subscribers to:

- Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent the use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.3 Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The Standard for private key protection for Administrators using such a cryptographic module requires them to:

- Use the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator's authorization.

6.2.8.4 Private Keys Held by Processing Centers (Class 1-3)

An online CA's private key is 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 are 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 removal from the token reader. ADACOM RA private keys (used for authentication to the RA application) are deactivated upon system log off. ADACOM RAs are required to log off their workstations when leaving their work area.

Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have the obligation to adequately protect their private key(s) in accordance with this CPS.

6.2.10 Method of Destroying Private Key

At the conclusion of an ADACOM CA's operational lifetime, one or more copies of the CA private key are archived in accordance with CPS § 6.2.5. Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple trusted individuals.

Where required, ADACOM destroys CA 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, CA key destruction activities are logged.

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 end-user Subscriber Certificates are backed up and archived as part of ADACOM' s routine backup procedures.

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 decryption and signature verification. The maximum Operational Periods for ADACOM Certificates for Certificates issued on or after the effective date of this CPS are set forth in the table below.

Certificate Issued By:	***Private Key Use***	***Validity Period***
Publicly Trusted Root CA (PCA)	No stipulation	Normally up to 25 years
ADACOM Issuing CA	No stipulation	Normally up to 15 years

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. The lifetime of Subscriber's certificates will not exceed the lifetime of the CA's signing certificate.

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 tokens containing ADACOM CA private keys is generated in accordance with the requirements of CPS § 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

ADACOM RAs are required to select strong passwords to protect their private keys. ADACOM's password selection guidelines require that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

ADACOM strongly recommends that Enterprise Administrators, RAs, and end-user Subscribers choose passwords that meet the same requirements. ADACOM also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

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

ADACOM RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser's "high security" option.

ADACOM strongly recommends that Client Administrators, RAs and end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

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, DigiCert PKI 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 shall be 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. Enterprise Customers must use Trustworthy Systems.

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.

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 in ADACOM's Production Operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by ADACOM in accordance with ADACOM systems development and change management standards. ADACOM also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with ADACOM system development standards.

DigiCert developed software, when first loaded, provides a method to verify that the software on the system originated from DigiCert or ADACOM, 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. DigiCert creates a hash of all software packages and DigiCert 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.

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 Information 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 secured networks 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 well as penetration tests on the PKI systems

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries contain time and date information.
The system time on ADACOM's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every one hour.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

ADACOM Certificates generally conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280").

At a minimum, X.509 Certificates shall contain the basic fields and indicated prescribed values or value constraints in the table below:

Field	***Value or Value constraint***
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See Section 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Encoded in accordance with RFC 5280.
Valid To	Universal Coordinate Time base. Encoded in accordance with RFC 5280.
Subject DN	See Section 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

7.1.1 Version Number(s)

ADACOM Certificates are X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. ADACOM intermediate and issuing CA certificates are X.509 Version 3 CA Certificates. End-user Subscriber Certificates are X.509 Version 3.

7.1.2 Certificate Extensions

ADACOM populates X.509 Version 3 Certificates with the extensions required by Section 7.1.2.1-7.1.2.8. Private extensions are permissible, but the use of private extensions is not warranted under this CPS unless specifically included by reference.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The criticality field of the KeyUsage extension is set to TRUE for CA certificates and set to FALSE for Class 1 and 2

Note: The nonRepudiation bit[11] is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the nonRepudiation bit means. Until such a consensus emerges, the nonRepudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the nonRepudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision. Consequently, this CPS does not require that the nonRepudiation bit be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager, or as otherwise requested. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). DigiCert and ADACOM shall incur no liability in relation thereto.

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier for the DigiCert CP in accordance with CP and this CPS Section 7.1.6 and with policy qualifiers set forth in CP and this CPS Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of X.509 Version 3 Certificates are populated in accordance with RFC 5280 with the exception of those issued under Public Lite accounts which may optionally exclude the email address in SubjAltName. The criticality field of this extension is set to FALSE.

7.1.2.4 Basic Constraints

ADACOM X.509 Version 3 CA Certificates BasicConstraints extension have the CA field set to TRUE. End-user Subscriber Certificates BasicConstraints extension, shall have the CA field set to FALSE. The criticality field of this extension is set to TRUE for CA Certificates, but may be set to TRUE or FALSE for end-user Subscriber Certificates.

ADACOM X.509 Version 3 CA Certificates have a “pathLenConstraint” field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to an online Enterprise Customer issuing end-user Subscriber Certificates have a “pathLenConstraint” field set to a value of “0” indicating that only an end-user Subscriber Certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

By default, ExtendedKeyUsage is set as a non-critical extension. DigiCert CA Certificates do not include the ExtendedKeyUsage extension

7.1.2.6 CRL Distribution Points

All ADACOM X.509 Version 3 end user Subscriber Certificates and Intermediate and Issuing CA Certificates include the cRLDistributionPoints extension containing the URL of the location where

[11] The nonRepudiation bit may also be referred to as ContentCommitment in Digital Certificates in accordance with the X.509 standard.

a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

ADACOM generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Where ADACOM populates X.509 Version 3 Certificates with a subjectKeyIdentifier extension.the keyIdentifier based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

CA certificates of an Enterprise Customer may include the Subject Key Identifier extension.

7.1.3 Algorithm Object Identifiers

ADACOM Certificates are signed using the following algorithm:

- **sha-1WithRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- **sha-2WithRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificate signatures produced using these algorithms shall comply with RFC 3279.

7.1.4 Name Forms

ADACOM populates DigiCert Certificates with an Issuer and Subject Distinguished Name in accordance with Section 3.1.1.

In addition, ADACOM includes within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement are permitted only for Enterprise Customers, when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended, or if a pointer to the applicable Relying Party Agreement is included in the policy extension of the certificate.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in the DigiCert CP Section 1.2.
More specifically, DigiCert, acting as the policy-defining authority, has assigned an object identifier value extension for each Class of Certificate issued under DigiCert. The object identifier values used for the Classes of end-user Subscriber Certificates are:

- The Class 1 Certificate Policy: Symantec/pki/policies/stn-cp/class1 (2.16.840.1.113733.1.7.23.1).
- The Class 2 Certificate Policy: Symantec/pki/policies/stn-cp/class2 (2.16.840.1.113733.1.7.23.2).[12]

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

ADACOM generally populates X.509 Version 3 Certificates with a policy qualifier within the Certificate Policies extension. Such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the ADACOM CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

CRLs contain the basic fields and contents specified in the table below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL Algorithm used to sign the CRL in accordance with RFC 3279. ADACOM CRLs are signed using sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
Issuer	Entity that has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.4.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

[12] It is used for Enterprise Customers.

7.2.1 Version Number(s)

ADACOM supports both X.509 Version1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 5280.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate.
ADACOM may provide OCSP services for its Enterprise certificates or the certificates that issue. OCSP responders conform to RFC 2560.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC 2560 is supported.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

An annual audit is performed for ADACOM's data center operations and key management operations supporting ADACOM's public and Enterprise Customer's CA services. Customer-specific CAs are not specifically audited as part of the audit of ADACOM's operations unless required by the Customer. ADACOM shall be entitled to require that Enterprise Customers undergo a compliance audit under this CPS and audit programs for these types of Customers.

In addition to compliance audits, ADACOM is entitled to perform other reviews and investigations to ensure the trustworthiness of ADACOM's Sub-domain of the DigiCert PKI, which include, but are not limited to:

- ADACOM is entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself or a Customer in the event ADACOM has reason to believe that the audited entity has failed to meet DigiCert Policies, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the DigiCert PKI.
- ADACOM is entitled to perform "Supplemental Risk Management Reviews" on itself or a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

ADACOM is entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with ADACOM and the personnel performing the audit, review, or investigation.

Additionally, a periodic compliance, with the Greek law and this CPS, audit is performed, by the control bodies that are designated from the Hellenic Telecommunications and Post Commission, in accordance with the Greek law.

8.1 Frequency and Circumstances of Assessment

ADACOM Compliance Audits are conducted at least annually. ADACOM customer audits are conducted at the sole expense of the audited entity.

8.2 Identity/Qualifications of Assessor

ADACOM's CA compliance audits are performed by:

- ADACOM internally, by Qualified IT Auditors, and
- the Hellenic Telecommunications and Post Commission (Supervisory Body) or the bodies designated by it, have the right to perform audits pursuant to applicable law or
- An auditing firm that demonstrates proficiency in public key infrastructure technology, information security tools and techniques and security auditing.

8.3 Topics Covered by Assessment

The scope of ADACOM's annual audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.4 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 DigiCert PKI, 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.

8.5 Communications of Results

Results of the compliance audit of ADACOM's operations may be released at the discretion of ADACOM's Management.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

ADACOM charges end-user Subscribers for the issuance, management, and renewal 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 making the CRLs required by this CPS available in a repository or otherwise available to Relying Parties. ADACOM is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. ADACOM does not permit access to revocation information, Certificate status information, or time stamping 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

9.5.5.1 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 gc@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.

9.5.5.2 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 error and omission insurance coverage. Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

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. Enterprise Customers must have sufficient financial resources to maintain their operations and perform their duties, as well, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by enterprise Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by ADACOM or a Customer,
- Audit reports created by ADACOM or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of ADACOM hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, ADACOM repositories and information contained within them are not considered Confidential Information. Information not expressly deemed Confidential Information under Section 9.3.1 is not considered confidential. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

ADACOM secures private information from compromise and disclosure to third parties.

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 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 Greek laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

ADACOM and all its Sub-domain participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all privacy laws in their jurisdiction.

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 is not used without the consent of the party to whom that information applies, in accordance with applicable privacy law.

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 Confidential 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 Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such ADACOM Sub-domain Participants. The following subsections of Section 9.5 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 and Customers grant 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 Relying Party Agreement referenced in the Certificate. ADACOM and Customers grant permission to use revocation information to perform Relying Party functions subject to the applicable Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

DigiCert PKI Participants 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 end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Managed PKI Key Manager, 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, DigiCert's Root public keys and the Root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of DigiCert. DigiCert 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 DigiCert or ADACOM.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

ADACOM 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 or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.2 RA Representations and Warranties

RAs warrant 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.

RA Agreement may include additional representations and warranties.

.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and 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.

Subscriber Agreement may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

ADACOM Relying Party Agreements 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. Any unauthorized reliance on a Certificate is at a party's own risk.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

ADACOM provides limited warranties and disclaims all other warranties, including warranties of

merchantability or fitness for a particular purpose, limits liability, and excludes all liability, except in case of willful misconduct or gross negligence, for any loss of profits, loss of data, or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, performance, nonperformance, or unavailability of certificates, electronic signatures, electronic seals, time stamps or any other transactions or services offered or contemplated herein, even if ADACOM has been advised of the possibility of such damages.

9.8 Limitations of Liability

EXCEPT AS STATED ABOVE, ANY ENTITY USING AN ADACOM CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF ADACOM RELATED TO SUCH USE, PROVIDED THAT ADACOM HAS MATERIALLY COMPLIED WITH THIS CPS IN PROVIDING THE CERTIFICATE OR SERVICE.

All liability is limited to actual and legally provable damages. ADACOM is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if ADACOM is aware of the possibility of such damages;
2. Liability related to fraud or willful misconduct of the Subscriber;
3. Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CPS;
4. Liability related to the security, usability, or integrity of products not supplied by ADACOM; or
5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether ADACOM failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of ADACOM'S Certificates.

To the extent ADACOM has issued and managed the Certificate(s) at issue in compliance with this CP and its CPS, ADACOM shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s).

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber Agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

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 applicable Subscriber agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

Relying Party Agreements require 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 applicable Relying Party agreement 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.

ADACOM will notify DigiCert according to the CA/B Forum notification requirements, in case of:
1. Changes in Certificate issuance procedures regarding certificates containing email address;
2. Terminations or transition of ownership of ADACOM CAs;
3. Ownership or control of the CA certificates changes;
4. There is a material change in ADACOM's operations (i.e. when the cryptographic hardware is consequently moved from one secure location to another.)

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 are published at http://pki.adacom.com/repository Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA determines whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

9.12.2 Notification Mechanism and Period

ADACOM reserve 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.

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 PKI 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 Version History 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 DigiCert, 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 corresponding to each Class of Certificate. Otherwise, amendments do not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among ADACOM, Affiliates, and Customers

Disputes among ADACOM PKI participants are resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

ADACOM Subscriber Agreements and Relying Party Agreements 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

This CPS is subject to applicable Greek and European law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

Not applicable.

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)

Not applicable.

9.16.5 Force Majeure

ADACOM Subscriber Agreements and Relying Party Agreements may include a force majeure clause protecting ADACOM.

9.17 Other Provisions

Not applicable.

Appendix A. Table of Acronyms and definitions

Table of Acronyms

Term	Definition
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
FIPS	United State Federal Information Processing Standards.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SSL	Secure Sockets Layer.

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center or Managed PKI Customer, that performs validation and other CA or RA functions.
ADACOM Practices Development Group	The organization within ADACOM, responsible for promulgating this policy throughout the ADACOM Sub-domain.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with DigiCert to be a DigiCert distribution and services channel within a specific territory.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Policies (CP)	The document which is the principal statement of policy governing the DigiCert PKI.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally

Term	Definition
	indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the DigiCert PKI.
Certification Practice Statement (CPS)	This document which states the practices that ADACOM employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	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 or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is ADACOM providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center or Managed PKI Customer undergoes to determine its conformance with DigiCert Policies that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
DigiCert	Means DigiCert Inc. and/or any wholly owned DigiCert subsidiary responsible for the specific operations at issue.
DigiCert PKI Participant	An individual or organization that is one or more of the following within the DigiCert PKI: DigiCert, ADACOM, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
Enterprise	A line of business that ADACOM enters to provide Managed PKI services to Managed PKI Customers.
Exigent Audit/Investigation	An audit or investigation by DigiCert or ADACOM where ADACOM has reason to believe that an entity failure to meet DigiCert's Policies, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the DigiCert PKI posed by the entity has occurred.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	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.
Key Generation Ceremony	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.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
Managed PKI	ADACOM 's fully integrated managed PKI service that allows enterprise Customers of ADACOM to distribute Certificates to individuals, such as employees, partners, suppliers, and customers. Managed PKI permits enterprises to secure messaging, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for an Managed PKI Customer.

Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	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 an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	DigiCert 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.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within ADACOM responsible for managing, reviewing, updating and approving this document.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	The ADACOM site that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the DigiCert PKI and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The DigiCert PKI consists of systems that collaborate to provide and implement the DigiCert PKI.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.

Secret Share	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.
Secret Sharing	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 under CP § 6.2.2.
Secure Sockets Layer (SSL)	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.
Service Center	The ADACOM operation that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Sub-domain	The portion of the DigiCert PKI under control of an entity and all entities subordinate to it within the DigiCert PKI hierarchy.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a DigiCert PKI hierarchy (the Class 1, or 3 hierarchy).
Reseller	An entity marketing services on behalf of ADACOM to specific markets.
Trusted Person	An employee, contractor, or consultant of an entity within the DigiCert PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a DigiCert PKI entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
ADACOM Repository	ADACOM's database of Certificates and other relevant ADACOM Sub-domain information accessible on-line.