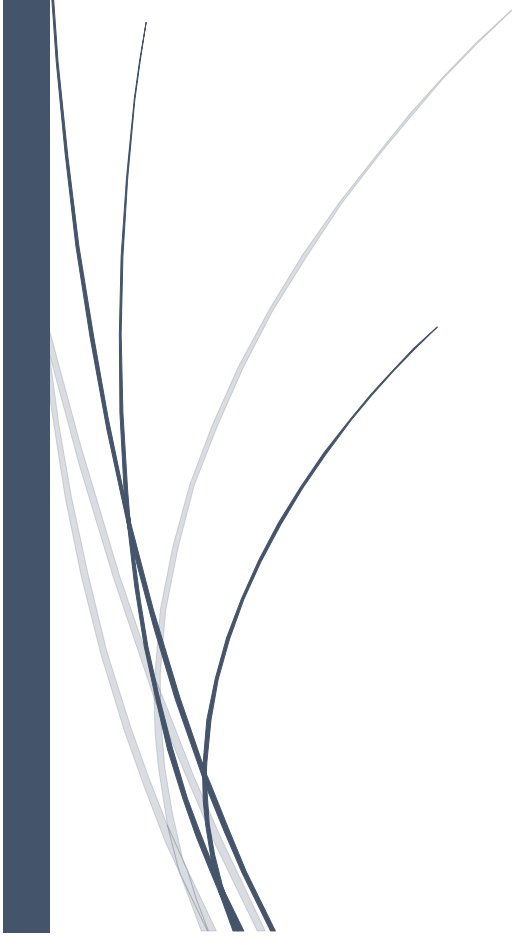
11-2-2022

Certification Practice Statement (CPS)

Publicly Trusted Certificates

Version 2.0



EADTrust Policy Committee
EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST S.L.

Copyright notice

Document versions

This publication could include technical inaccuracies or typographical errors.

As the state of the technique and legislative context evolves, it may be necessary to include changes to this document, so please check the EADTrust website for the latest version of the publication.

European Agency of Digital Trust may make improvements and changes in the products and the programs described in this publication at any time.

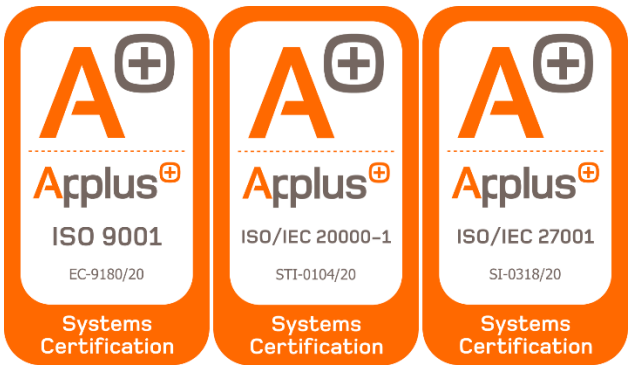
Certification ISO 9001, ISO 27001 and ISO 20000-1

EADTrust has passed several audits, and in particular those related to the ISO 9001, ISO 27001 and ISO 20000-1 standards, with the following scope:

> *The Integrated Information Management System that supports consulting, auditing, development and provision of the following electronic trust services: Certification Authorities (PKI) that meet the requirements of EN 319 401 v2.2.1, EN 319 411-1 v1.2.2, EN 319 411-2 v2.2.2, EN 319 421 v1.1. 1 for Time Stamping, Certificate Issuance, OCSP Validation, Centralized Electronic Signature, Electronic Signature Extension, Certified Electronic Notification (Certified Electronic Mail), Certified Electronic Publishing, Digital Content Proofing, Electronic Shareholders' Forum, Key Issuance and Management, Cartulario (Digital Custody of Electronic Documents), Electronic Evidence Custody (Data Retention), Electronic Voting, Electronic Invoicing, Certified Digitalization, Digitalized Handwritten Signature Management and Vocal Advanced Signature Management, to guarantee the legal validity of all types of transactions that use them, in accordance with the declaration of applicability in force.*

Certificates:

Standard	Certificate
ISO/IEC 20000-1	STI-0104/20
ISO/IEC 27001	SI-0318/20
ISO 9001	EC-9180/20



Qualified Trust Service Provider

EADTrust has passed the annual audit for Publicly Trusted Certificates in accordance with REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, which qualifies it for the following services: issuance of Qualified Certificate for Electronic Signature (Art. 28 of the eIDAS Regulation), Qualified Certificate for Electronic Seal (Art. 38 of the eIDAS Regulation), Qualified Certificate for Website Authentication (Art. 45 of the eIDAS Regulation), Qualified electronic Timestamps (Art. 42 of the eIDAS Regulation).

CSQA Certificazioni (eadtRUST Conformity Assessment Body) has assigned the certificate number **58813**.

The Spanish Ministry of Economic Affairs and Digital Transformation has published a Trusted Service List (TSL) corresponding to providers that issue qualified electronic certificates and are established and supervised in Spain, in line with the aforementioned legislation. EADTrust was included in this list on October 7, 2020.

INDEX

1. INTRODUCTION

1.1 Documentary control

Version	Date	Substituted documents	Description
1.0	May 2021	None	EADTrusts Publicly Trusted Certificate certification practice statement (CPS).
1.1	June 2021	Version 1	Non-qualified DV, OV, EV profiles are introduced and the informative OU of the type of certificate, the keyusage, key encipherment (an error occurs with the ECDSA keys in the link) and the userNotices are removed from all the web profiles except in the electronic office, which is given by the electronic profiles document of the Ministry of Finance and Public Administrations.
2.0	February 2022	Version 1.1	Extensive changes separating DPC for qualified certificates issued to natural persons to sign electronically and to legal persons to seal electronically, apart from this CPS devoted only to Publicly Trusted Certificates.

Document properties	
Owner	EADTrust European Agency of Digital Trust, S.L.
Date	February the 11th, 2022
Distribution	Public
Name / Code	Publicly-Trusted-Certificates-EADTrust-CPS (V2.0)

1.2 Overview

This Certification Practice Statement ("CPS") document outlines the certification services practices for European Agency of Digital Trust, S.L. (“EADTrust”) Public Key Infrastructure ("PKI").

EADTrust PKI services include, but are not limited to, issuing, managing, validating, revoking, and renewing Certificates in accordance with the requirements of the EADTrust Certificate Policy (CP). It is recommended that readers familiarize themselves with the EADTrust CP prior to reading this document.

The EADTrust PKI conforms to the current version of the guidelines adopted by the Certification Authority/Browser Forum (“CAB Forum”) when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates (“Baseline Requirements”). CAB Forum documents can be found at https://www.cabforum.org. If there is any conflict between this CPS and a relevant CAB Forum requirement or guideline, then the CAB Forum requirement or guideline shall take precedence.

Other documents related to the behavior and control of the EADTrust PKI, such as a Subscriber Agreement and Privacy Policy, can be found at https://eadtrust.eu/documentos-vigentes/.

Per IETF PKIX RFC 3647, this CPS is divided into nine components that cover security controls, practices, and procedures for certification services provided by the EADTRUST PKI.

The following Certification Authorities are covered under this CPS:

CA Type	Distinguished Name	Key Pair Type and Parameters	Cert Fingerprint	Validity Period
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019	ECDSA, curve P-256	e0:16:ad:b4:3e:92:83:9e:8a:dd:93:c6:fd:26:93:ce:e2:f4:8d:13	Not Before: Jun 6 13:35:52 2019 GMT, Not After: May 31 13:35:52 2043 GMT
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019	ECDSA, curve P-256	48:52:9a:b1:76:ea:39:b4:f5:4c:5d:c9:41:00:a5:0c:a6:52:b3:dd	Not Before: Jun 6 13:49:24 2019 GMT, Not After: May 31 13:49:24 2043 GMT
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust ECC 384 Root CA For Qualified Web DV/OV Cert 2019	ECDSA, curve P-384	3b:0e:52:7b:93:52:6d:dc:08:45:dd:6b:c3:75:d0:bd:99:f2:a4:ac	Not Before: Jun 6 13:35:55 2019 GMT, Not After: May 31 13:35:55 2043 GMT
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust ECC 384 Root CA For Qualified Web EV/PSD2 Cert 2019	ECDSA, curve P-384	1b:07:bd:9d:d7:48:7b:b8:d6:a7:18:a6:60:77:b9:a1:8b:87:d1:8a	Not Before: Jun 6 13:49:26 2019 GMT, Not After: May 31 13:49:26 2043 GMT
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust RSA 4096 Root CA For	RSA, 4096 bits, 05 00	09:ec:23:59:75:94:a2:bc:4c:9f:c3:23:51:14:34:a7:bc:5f:4e:d8	Not Before: Jun 6 13:23:34 2019 GMT, Not After: May 31 13:23:34 2043 GMT

CA Type	Distinguished Name	Key Pair Type and Parameters	Cert Fingerprint	Validity Period
	Qualified Web DV/OV Cert 2019			
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust RSA 4096 Root CA For Qualified Web EV/PSD2 Cert 2019	RSA, 4096 bits, 05 00	a5:9f:a6:30:d8:b6:2c:93: ee:2c:51:0a:f5:52:82:2a: 87:57:17:07	Not Before: Jun 6 13:36:31 2019 GMT, Not After: May 31 13:36:31 2043 GMT
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust RSA 8192 Root CA For Qualified Web DV/OV Cert 2019	RSA, 8192 bits, 05 00	13:ff:6d:56:9a:8b:a6:be: 55:a5:6c:1b:ae:82:ae:3c: f2:c6:63:ff	Not Before: Jun 6 13:28:28 2019 GMT, Not After: May 31 13:28:28 2043 GMT
Root CA	C=ES, O=European Agency of Digital Trust, S.L., CN=EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019	RSA, 8192 bits, 05 00	c5:e3:44:8a:aa:cb:e1:cb: ec:4f:39:c8:36:54:d6:1f:f8: df:be:82	Not Before: Jun 6 13:45:37 2019 GMT, Not After: May 31 13:45:37 2043 GMT

1.3 Document name and identification

This is the EADTrust Certification Practices Statement for web services (Publicly Trusted Certificates EADTrust CPS). This document was approved for publication by the EADTrust Policy Management Authority, and is made available at https://eadtrust.eu/en/documents-in-force/

In addition to this CPS there is another CPS that includes the rest of the trust services provided by EADTrust, which can be consulted at: https://eadtrust.eu/en/documents-in-force/

1.4 PKI participants

1.4.1 Certification authority

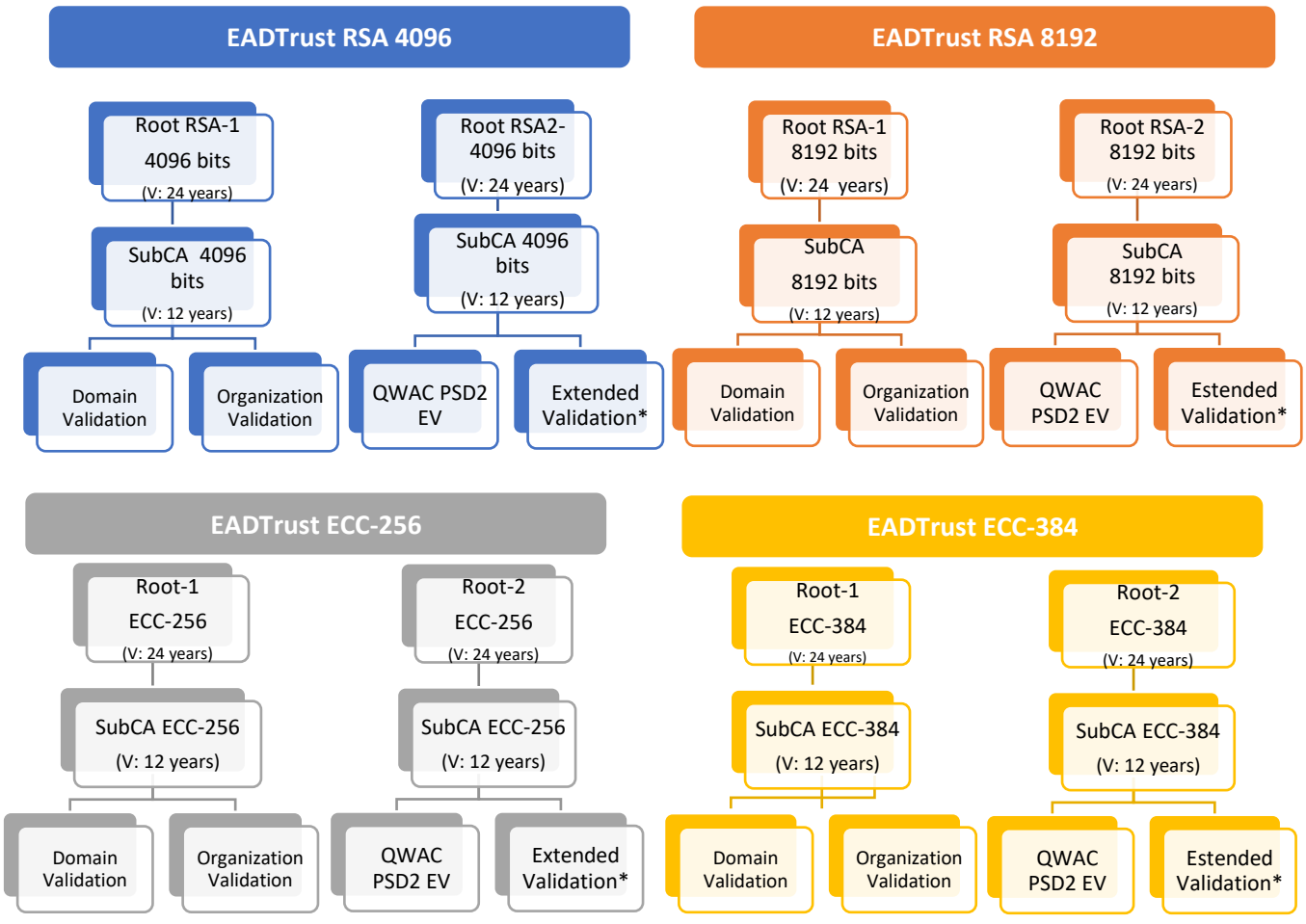
EADTrust is a CA that provides services including, but not limited to, issuing, managing, validating, revoking, and renewing publicly-trusted Certificates. These services are performed in accordance with the requirements of the EADTrust Certificate Policy (CP) and this CPS. These

services are provided to the general public with exceptions as deemed appropriate by EADTrust management or in accordance with relevant law.

The CAs are organized in a two-tier hierarchy, with several offline root CAs, adapted to current industry standards and practices, from a technological point of view:

- RSA Root CA Web 4096-bit key size with SHA256 digest algorithm (Domain and Organization Validated).
- RSA Root CA Web 8192-bit key size with SHA512 digest algorithm (Domain and Organization Validated).
- ECC Root CA Web P-256 with SHA256 digest algorithm (Domain and Organization Validated).
- ECC Root CA Web P-384 with SHA384 digest algorithm (Domain and Organization Validated).
- RSA Root CA Web 4096-bit key size with SHA256 digest algorithm (Extended Validation and PSD2).
- RSA Root CA Web 8192-bit key size with SHA512 digest algorithm (Extended Validation and PSD2).
- ECC Root CA Web P-256 with SHA256 digest algorithm (Extended Validation and PSD2).
- ECC Root CA Web P-384 with SHA384digest algorithm (Extended Validation and PSD2).

- **Qualified Root's for Web:**



1.4.2 Registration authorities

EADTrust, as a CA, issues some certificates directly using its own Registration Authority (RA). However, as a service company, the certificate market is usually reached through Registration Authorities operated by external organizations.

RAs cooperating in the EADTrust hierarchy are required to comply with all EADTrust Certification Policies, as well as pass the mandatory annual compliance assessment conducted by EADTrust or any third-party assessor or auditor appointed by EADTrust.

1.4.3 Subscribers

The subscriber of a certificate is the natural or legal person who contracts the certificate issuance service.

In individual certificates, the subscriber and the owner of the key coincide. In certificates in which both figures do not coincide (such as entities and organization certificates), the subscriber is usually a legal entity, and the key owner is a natural person, representative or employee authorized by the organization to receive and use the certificate. In this case, not only the subscriber will sign the corresponding agreement, but also each of the certificate owners will receive and sign the document informing them of their obligations when they identify themselves to the RA.

1.4.4 Relying parties

Entities or individuals acting in reliance on certificates or signed objects issued under this PKI are relying parties.

Relying parties access the certificate under an SSL/TLS connection and should verify the validity of the certificate and its purpose.

They should verify by the Authority Information Access (AIA) field of the certificates that they can reconstruct the chain of trust from the end-entity certificate to the Root authority, and that they can identify the certificate validity query point by the OCSP service, or, where applicable, by the CRL list.

1.4.5 Other participants

No stipulation.

1.5 Certificate usage

1.5.1 Appropriate certificate uses

Web authentication certificates will be used to encrypt communications between the browser and the web server and identify the domain and the domain owner. In the case of electronic site certificates, they can be used to provide the site with SSL/TSL capabilities.

This type of certificate can also be used to sign authentication messages, in particular TLS client challenges. This technical digital signature is used to guarantee the identity of the certificate subscriber but does not express conformity with what is signed. Qualified certificates conform to the technical standard EN 319 412 (documents 1 to 5) of the European Telecommunications Standards Institute ETSI.

1.5.2 Prohibited certificate uses

Certificates must be used for the specific purpose for which they were created.

Certificates must also only be used in accordance with applicable law.

Certificates may not be used:

- For any application requiring fail-safe performance such as a) the operation of nuclear power facilities b) air traffic control systems c) aircraft navigation systems d) weapons control systems e) any other system in which failure could lead to injury, death, or environmental damage.
- For software or hardware architectures that provide facilities for interference with encrypted communications, including but not limited to a) active eavesdropping (e.g., Man-in-the-middle attacks) b) traffic management of domain names or internet protocol (IP) addresses that the organization does not own or control. Note that these restrictions shall apply regardless of whether a relying party communicating through the software or hardware architecture has knowledge of its providing facilities for interference with encrypted communications.

Note that Certificates do not guarantee anything regarding reputation, honesty, or the current state of endpoint security. A Certificate only represents that the information contained in it was verified as reasonably correct when the Certificate was issued.

EADTrust incorporates in the certificate information about the limitation of use, in standardized fields in the attributes "Key usage" and "Extended Key Usage".

1.6 Policy administration

1.6.1 Organization administering the document

EADTrust, with registered office at Calle Mentrida, 6, Madrid (Spain) and Tax Identification Number B-85626240, is the Certification Authority that issues the certificates under this Certification Practice Statement (CPS).

1.6.2 Contact person

The EADTrust PMA can be contacted at:

Policy Management Authority
European Agency of Digital Trust, S.L.
Calle Méntrida 6
Madrid, Spain 28043

Certificate Problem Reports can be submitted via email to:

info@eadtrust.eu

1.6.3 Person determining CPS suitability for the policy

The EADTrust PMA is responsible for determining the suitability of this CPS. The EADTrust PMA is informed by results and recommendations received from an independent auditor.

1.6.4 CPS approval procedures

The EADTrust PMA approves any revisions to this CPS document after formal review.

The Certificate Policy Approval and Management Body can be contacted at: policy@eadtrust.eu.

1.7 Definitions and acronyms

1.7.1 Definitions

- Applicant
  - An entity applying for a certificate.
- Affiliate
  - A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, or any entity operating under the direct control of a Government Entity
- Application Software Supplier
  - A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates EADTrust Root Certificates.
- Audit Period
  - In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement.
- Baseline Requirements
  - A document published by the CAB Forum which outlines minimum requirements for publicly trusted Certificate Authorities.
- CA Certificate
  - A Certificate in which the basic Constraints field has the CA attribute set to TRUE.
- CAA
  - From RFC 8659: "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue".
- CAB Forum

  - Certificate Authority / Browser Forum, a group a CAs and browsers which come together to discuss technical and policy issues related to PKI systems. (https://cabforum.org/)
- Certificate for Electronic Signature
  - An electronic document that uses a digital signature to bind a public key and an identity.
- Certificate Policy
  - A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- Certificate Problem Report
  - Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
- Certificate Profile
  - A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 or a certificate template file used by CA software.
- Certificate Repository
  - A repository of information about EADTrust certificates. It is located at: https://eadtrust.eu/en/documents-in-force/
- Certificate Revocation List
  - A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
- Certificate Transparency
  - An "append-only" public logging Certificate system as described by RFC 6962.
- Certification Authority
  - An organization that is responsible for the creation, issuance, revocation, and management of Certificates
- Certification Practice Statement
  - One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- Country
  - Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.
- Cross Certificate
  - A certificate that is used to establish a trust relationship between two Root CAs.
- Domain Name
  - The label assigned to a node in the Domain Name System.
- EV Certificate
  - A certificate that contains subject information specified in, and which has been validated in accordance with the EV Guidelines. There are EV Certificates for SSL/TLS and for Code Signing. Both certificate types follow the same practices for validation Subject Information related to the Identity of the Applicant.
- Expiry Data
  - The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
- Fully-Qualified Domain Name

  - A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
- Government Agency
  - In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.
- Government Entity
  - A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
- Incorporating Agency
  - In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.
- Issuing CA
  - In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
- Jurisdiction of Incorporation
  - In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
- Key Compromise
  - A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
- Key Pair
  - A Private Key and its associated Public Key.
- Notary
  - A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document.
- Object Identifier
  - A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
- OCSP Responder
  - An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests

and providing Online Certificate Status Protocol responses. See also, Online Certificate Status Protocol.

- Online Certificate Status Protocol
  - An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.
- Penetration Test
  - A process that identifies and attempts to exploit openings and vulnerabilities on the Certificate System through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.
- Policy and Legal Repository
  - A repository of policy and legal documents related to the EADTrust PKI. It is located at: http://eadtrust.rgpd.de/en/privacy-policy/
- Private Key
  - The key in a Key Pair that must be kept secret. Used to create digital signatures that can be verified by the corresponding Public Key or to decrypt messages encrypted by the corresponding Public Key.
- Private Organization
  - A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.
- Public Key
  - The only key in a Key Pair that can safely be publicly disclosed. Used by Relying Parties to verify digital signatures from the corresponding private key or to encrypt messages that can only be decrypted by the corresponding private key.
- Public Key Infrastructure
  - A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
- Publicly Trusted Certificate
  - A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
- Registration Number
  - The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation.
- Registration Authority
  - Any Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- Relying Party
  - An entity that relies upon information contained within certificates issued by EADTrust PKI services.

- Root CA
  - The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- Secure PKI Facilities
  - Facilities designed to protect sensitive PKI infrastructure, including CA private keys.
- Subject
  - The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- Subordinate CA
  - A Certification Authority in possession or control of the Private Key associated with a Subordinate CA Certificate. A Subordinate CA Operator is either an Externally Operated Subordinate CA or an Internally Operated Subordinate CA.
- Subordinate CA Certificate
  - A CA Certificate that has been signed by the Private Key associated with a Root CA Certificate or a different Subordinate CA Certificate
- Subscriber
  - An entity that has agreed to a Subscriber Agreement and is using EADTrust PKI services.
- Subscriber Agreement
  - An agreement between EADTrust and the Applicant/Subscriber that specifies the rights and responsibilities of the parties
- Terms of Use
  - Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with this CP/CPS when the Applicant/Subscriber is an Affiliate of EADTrust or IS EADTrust.
- Time-Stamp
  - Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.
- Trusted Contributor
  - A contributor who performs in a Trusted Role. Trusted Contributors may be employees, contractors, or community members. Trusted Contributors must be properly trained and qualified, and have the proper legal obligations in place before performing in a Trusted Role.
- Trusted Role
  - A role which qualifies a person to access or modify EADTrust PKI systems, infrastructure, and confidential information.
- Valid Certificate
  - A Certificate that passes the validation procedure specified in RFC 5280.
- Validity Period (of a certificate)
  - The period of time from notBefore through notAfter, inclusive.
- Vulnerability scan
  - A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities.

- WHOIS
    - Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
- Wildcard Certificate
    - A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

1.7.2 Acronyms

CA	Certificate Authority
CAA	Certificate Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CT	Certificate Transparency
DN	Distinguished Name
DV	Domain Validation
DVCP	Domain Validation Certificates Policy
EADTrust	European Agency of Digital Trust
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic Identification, Authentication and trust Services
EKU	Extended Key Usage
EV	Extended Validation
EVCP	Extended Validation Certificates Policy
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IDN	Internationalized Domain Name
IP	Internet Protocol
ISO	International Organization of Standardization
OCSP	On-line Certificate Status Protocol
OID	International Standards Organization's Object Identifier
OV	Organization Validated
OVCP	Organization Validation Certificates Policy
PIN	Personal identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	IETF Working Group on PKI
PMA	Policy Management Authority
PSD2	Payment Services Directive
QSeal	Qualified electronic Seal Certificate
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
SSL	Secure Socket Layer

SubCA	Subordinate Certification Authority
TLD	Top Level Domain
TLS	Transport Layer Security
TSL	Trusted Service List
TSP	Trust Service Provider
URL	Uniform Resource Locator
X.509	ITU-T standard for Certificates and authentication framework

1.7.3 Conventions

Terms not otherwise defined in this CPS shall be as defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of the CA.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The CA provides revocation information for Subordinate Certificates and Subscriber Certificates available under this CPS.

The URL where the revocation information is available (and indicated in the AIA field of the certificate) is:

- ocsp.eadtrust.eu

In addition, possible revocation of root CAs and subordinate CAs will be recorded at the URL:

- https://crl.eadtrust.eu

The certification policies, the certification practice statement and the abbreviated Policy Disclosure Statement (PDS) will be available at the URL:

- https://eadtrust.eu/en/documents-in-force/

2.2 Publication of certification information

Records of all EADTrust root and intermediate certificates, including those that have been revoked, are available in the Certificate Repository:

https://eadtrust.eu/en/documents-in-force/

The disclosure includes all material required by RFC 3647 and is structured in accordance with that standard.

The CA for issuing certificates for SSL/TLS conforms to the current version of the Basic Requirements for the Issuance and Management of Publicly Trusted Certificates published at: http://www.cabforum.org. In the event of any inconsistency between this document and the Requirements, the Requirements shall prevail over this document.

EADTrust hosts testing web pages that allow Application Software Providers to test their software with Subscriber Certificates that chain each publicly trusted Root Certificate.

EADTrust hosts separate websites using Subscriber Certificates of various types: (i) valid, (ii) revoked and (iii) expired.

The domains of the test web sites respond to this structure:

- https://ecc-256-dv-tst.eadtrust.eu/
- https://ecc-256-dv-q-tst.eadtrust.eu/
- https://ecc-256-ev-tst.eadtrust.eu/
- https://ecc-256-ev-q-tst.eadtrust.eu/
- https://ecc-256-ov-tst.eadtrust.eu/
- https://ecc-256-psd2-tst.eadtrust.eu/
- https://ecc-384-dv-tst.eadtrust.eu/
- https://ecc-384-dv-q-tst.eadtrust.eu/
- https://ecc-384-ev-tst.eadtrust.eu/
- https://ecc-384-ev-q-tst.eadtrust.eu/
- https://ecc-384-ov-tst.eadtrust.eu/
- https://ecc-384-psd2-tst.eadtrust.eu/
- https://rsa-2048-dv-tst.eadtrust.eu/
- https://rsa-2048-dv-q-tst.eadtrust.eu/
- https://rsa-2048-ev-tst.eadtrust.eu/
- https://rsa-2048-ev-q-tst.eadtrust.eu/
- https://rsa-2048-ov-tst.eadtrust.eu/
- https://rsa-2048-psd2-tst.eadtrust.eu/
- https://rsa-2048-evsedealto-tst.eadtrust.eu/
- https://rsa-4096-dv-tst.eadtrust.eu/
- https://rsa-4096-dv-q-tst.eadtrust.eu/
- https://rsa-4096-ev-tst.eadtrust.eu/
- https://rsa-4096-ev-q-tst.eadtrust.eu/
- https://rsa-4096-evsedealto-tst.eadtrust.eu/
- https://rsa-4096-ov-tst.eadtrust.eu/
- https://rsa-4096-psd2-tst.eadtrust.eu/
- https://rsa-8192-dv-tst.eadtrust.eu/
- https://rsa-8192-dv-q-tst.eadtrust.eu/
- https://rsa-8192-ev-tst.eadtrust.eu/
- https://rsa-8192-ev-q-tst.eadtrust.eu/
- https://rsa-8192-ov-tst.eadtrust.eu/
- https://rsa-8192-psd2-tst.eadtrust.eu/
- https://rsa-8192-evsedealto-tst.eadtrust.eu/

On port 443, the certificates in force are located. Revoked certificates that have not expired are located on port 8443, and in port 9443, the expired certificates.

E.g.: Domain Validated RSA-2048 certificates, we would have:

- https://rsa-2048-dv-tst.eadtrust.eu Certificates in force
- https://rsa-2048-dv-tst.eadtrust.eu:8443 Revoked certificates
- https://rsa-2048-dv-tst.eadtrust.eu:9443 Expired certificates

2.3 Time or frequency of publication

EADTrust is committed to develop, implement, enforce and update annually, its Certification Policies and Certification Practices Statement, as one of the elements associated with the annual audit. The update interval will be shorter when technical or legal changes occur that require an update.

The audits of the CA for the issuance of SSL/TLS certificates shall be annual.

2.4 Access controls on repositories

Read only access to the Policy and Legal Repository and certificate information is unrestricted. Write access is protected by logical and physical controls.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Certificate distinguished names and subject alternative names are compliant with the CP.

3.1.2 Need for names to be meaningful

The name of the subject and issuer contained in a certificate must be meaningful in the sense that the CA has evidence of the association between these names and the entities to which they belong.

Each digital certificate contains a unique set of unique name attributes. These attributes include a collection of the person's name, company name, organizational unit, and unique identifier.

3.1.3 Anonymity or pseudonymity of subscribers

There is no anonymity in EADTrust web certificates, subscribers must be identified as stated in section 3.2.

3.1.4 Rules for interpreting various name forms

EADTrust complies with the X.500 standard as referenced in ISO/IEC 9594 **Information technology - Open Systems Interconnection - TheDirectory: Public-key and attribute certificate frameworks**

- X.509 - ISO/IEC 9594-8
- X.520 - ISO/IEC 9594-6

3.1.5 Uniqueness of names

The names of the subscribers (considering the different attributes) are unique for each type of certificate within the EADTrust Certification Practice Statement.

3.1.6 Recognition, authentication, and role of trademarks

EADTrust reserves the right to make all decisions regarding Subscriber names in certificates. Entities requesting certificates will be required to demonstrate their right to use names (e.g., demonstrate control of a domain name), but trademark rights are not verified.

While EADTrust will comply with Spanish Law and associated legal orders, it is EADTrust's position that trademark enforcement responsibility for domain names should lie primarily with domain registrars and the legal system.

3.2 Initial identity validation

EADTrust may elect not to issue any certificate at its sole discretion.

3.2.1 Method to prove possession of private key

The applicant provides a PKCS#10 certificate request generated on its web server, which implies possession of the private key.

If the keys are delivered in a PKCS#12 (or PFX) file, the proof of possession of the private key is demonstrated by virtue of the trusted procedure of delivery and acceptance of the file and decryption key, which may make use of two-factor authentication communication techniques (e.g., an email or SMS) or a shared secret determined at the time of completing the certificate request.

3.2.2 Authentication of organization and domain identity

As part of the EADTrust authentication process, in the case of issuance of web server certificates, the organization name entered during enrolment is validated and entered in the appropriate field of the certificate.

The organization to which a certificate is attributed must be an active entity, confirmed by an official authority responsible for business registration within the specific jurisdiction (locality, state, country) indicated in the certificate request. The name of the registered organization and the claimed name must match verbatim. If abbreviations exist, they will only apply to the parts that identify the legal type of company or entity (S.A., S.L., S. COOP., LLC, Ltd). When the entities are not companies, the powers of attorney provided and publications of appointments in the official gazettes will be used as reference.

In addition, the ownership of the domain name will be checked to ensure that it corresponds to the organization, and confirmation will be requested from the e-mail addresses associated with the domain through the WHOIS service. EADTrust may also use other means to perform this verification.

If the entity makes use of extensions in its DNS that restrict the issuance of certificates to certain Certification Service Providers, EADTrust will only issue web server certificates if this preference is expressly indicated. EADTrust reviews the CAA (Certification Authority Authorization) records when checking Fully Qualified Domain data, leaving a record of the checking actions in its records and logs.

The domain attributed to the certificate will be verified according to the requirements defined in the "Baseline Requirements for the issuance and management of publicly-trusted certificates" and "Guidelines for the issuance and management of extended validation certificates" of CA/Browser Forum, in their latest versions.

3.2.3 Authentication of individual identity

The authentication of the subscribers will be carried out through its own or affiliated Registration Entities, verifying the identity documents by means of the certificate holder's personal appearance.

3.2.4 Non-verified subscriber information

Non-verified Applicant information is not included in EADTrust certificates.

3.2.5 Validation of authority

To validate the identity of a person claiming to represent an authority, it will be necessary to identify that person and his or her relationship with the organization he or she claims to represent. This verification of identity may be done by means of a signature through a natural or legal person's certificate by the representative, or through verification before a notary.

3.2.6 Criteria for interoperation

See Section 3.2.5

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

See Section 4.7.

3.3.2 Identification and authentication for re-key after revocation

See Section 4.7.

3.4 Identification and authentication for revocation request

Identification and authentication for revocation requests is performed by EADTrust in compliance with Section 4.9 of this document.

Identification and authentication are not required when revocation is being requested by EADTrust.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Natural persons representing legal entities owning a website who need: the use of encrypted communications on their website in order to confirm the identity of the domain. In the case of bids, the conditions established by the contracting authority will be taken into account.

Issuance will depend on proper validation and compliance with EADTrust policies.

4.1.2 Enrollment process and responsibilities

The tasks of identification and validation of the information in the certificate and validation and approval of the requests for issuance and revocation will be performed by the Registry Offices.

The enrollment process involves the following steps, in no particular order:

- Generating a key par using secure methods.
- Submitting a request for a certificate containing all necessary information, including the public key.
- Agreeing to the relevant Subscriber Agreement.

EADTrust's own Registration Offices or those of the user entities with which EADTrust signs the corresponding legal instrument shall assume the following obligations:

- Validate the identity and other personal details of the applicant, subscriber and key owner in the certificates or information relevant to the purpose of the certificates according to these procedures.
- Verify the ownership of the domain to the applicant.
- Maintain all information and documentation relating to certificates, and manage their issuance, renewal, revocation or reactivation.
- Notify EADTrust of certificate revocation requests with due diligence and in a quick and reliable manner.
- Allow EADTrust access to its procedural files and audit logs to perform its functions and maintain necessary information.
- Inform EADTrust of requests for issuance, and revocation; as well as, any other aspect related to certificates issued by EADTrust.
- Validate, with due diligence, the circumstances of revocation that may affect the validity of the certificate.
- Comply with the procedures established by EADTrust and with the legislation in force in this matter, in its management operations related to the issuance, renewal and revocation of certificates.
- Where appropriate, it may perform the function of making available to the key holder the technical procedures for the creation of signatures (private key) and verification of the electronic signature (public key).

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The identity of the applicant and the possession of the domain will be verified, following the guidelines established by the "Baseline Requirements for the issuance and management of publicly-trusted certificates" and "Guidelines for the issuance and management of extended validation certificates" of CA/Browser Forum, in their latest versions.

In the case of bids, the conditions established by the contracting authority shall be taken into account.

4.2.2 Approval or rejection of certificate applications

If the information is not correct, the RA will deny the application and will contact the applicant to explain the reason. If the information is correct, the certificate will be issued.

In the EADTrust certificate issuance process, dual controls are applied so that the decision to issue the certificate cannot be made by the same person who checks the information associated with the application.

In the process of issuing web certificates (extended validation, organization validation, domain validation) defined in this CPS, a third control is also applied to verify that the domain is under the exclusive control of the certificate applicant.

4.2.3 Time to process certificate applications

Once the information required in the certificate request process has been verified, the certificate can be issued. Once the subscriber's identity has been verified, the certificate issuance time is 24 hours on working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificates can be issued on a software support.

I. Procedure for issuing certificates issued through a software mechanism, with a private key generated by the applicant:

- Together with the application form, the applicant generates a key pair on his/her own computer and submits to EADTrust the certificate application in PKCS#10 format.
- The Registration Authority authenticates the validity of the documentation submitted by the applicant.
- After receiving the documentation, EADTrust issues the certificate, which must be inserted into the device on which the request was generated.

II. Procedure for issuing certificates issued through a software mechanism, with a private key generated by the Provider:

- The applicant generates the application form.
- The Registration Authority authenticates the validity of the documentation submitted by the applicant.

- After receiving the documentation, EADTrust issues the certificate linked to the private key, in encrypted PKCS#12 format, which can be inserted in any device, even if it is not the device on which the request was generated.
- The key that allows the decryption and installation of the PKCS#12 file is sent to the requestor by a different way than the delivery of the PKCS#12 file.
- EADTrust deletes the private key and the PKCS#12 file upon delivery to the requestor.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Generally, within 24 hours of requesting the certificate; unless in the process of identification and verification of identity the RA detects any irregularity to be corrected or that prevents the issuance of the certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

By signing the contract of general and particular conditions of the service, EADTrust understands that the Subscriber/Key Holder has accepted the conditions of use, obligations and duties specified in the clauses of the contract and therefore has accepted the certificate.

4.4.2 Publication of the certificate by the CA

Certificates will be registered when appropriate in the "Certificate Transparency" system from where they will be available to third parties. This is a security measure defined within the framework of the CAB Forum.

4.4.3 Notification of certificate issuance by the CA to other entities

EADTrust may publish website certificates (used in the context of securing communications using TLS protocols) according to the "CertificateTransparency" standard[1].

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber who has custody of the keys:

- Shall ensure the correct use and maintenance of the certificate storage media.
- Will provide EADTrust and its registration entities with complete and adequate information in accordance with the requirements of this CPS and specific policies, in particular regarding the registration procedure.
- Make proper use of the certificate and, in particular, comply with the limitations on the use of the certificate.
- Diligently safeguard the private key (whatever its medium, and even if it is a backup copy) and the key or PIN code that enables its activation to prevent unauthorized use.

[1] https://www.certificate-transparency.org/

- It shall notify EADTrust, and any other person the Subscriber believes may rely on the certificate, without reasonable delay, if any of the following occur:

  1. The Subscriber's private key has been lost, stolen, or potentially compromised.
  2. Control over the Subscriber's private key has been lost due to the activation data being compromised (e.g., cryptographic device PIN code) or due to other reasons.
  3. Inaccuracy or changes to the certificate content, as reported or suspected by the subscriber, requesting revocation of the certificate when such changes constitute grounds for revocation.

- Shall cease to use the private key at the end of the certificate's validity period.
- Refrain from supervising, interfering or reverse engineering the technical implementation of the certification services without the prior written approval of the Certification Authority.
- Refrain from intentionally compromising the security of the certification services.
- Refrain from using the private keys corresponding to the public keys included in the certificates in order to sign a certificate as if performing the function of a Certification Authority.
- Subscribers of qualified certificates that generate digital signatures using the private key corresponding to the public key included in the certificate must assume that such electronic signatures are equivalent to handwritten signatures, provided that a cryptographic device (qualified electronic signature creation device) is used, according to the provisions of the eIDAS Regulation.
- Subscribers of qualified certificates that generate digital seals using the private key corresponding to the public key included in the certificate must assume that such digital seals enjoy a presumption of data integrity and the correctness of the origin of the data to which the qualified electronic seal is linked, provided that a cryptographic device (qualified electronic seal creation device) is used, according to the provisions of the eIDAS Regulation.
- Pay the fees for the certification services requested under the terms and conditions provided by the CA, when the holder coincides with the subscriber.
- Authorize the CA, through the RA, to use the personal data provided by the holder to validate, verify and authenticate the identity declared by the holder.
- To request the revocation of the Certificate when any of the events foreseen in this policy and in the specific practices and legislation in force for the different statuses of the life cycle of the certificates are fulfilled.
- Understand and accept the terms and conditions of use of the certificate, and any modification made to them.
- Not to intentionally compromise the security of the certification services.
- All those derived from this CPS, the certificate policy and current legislation.

4.5.2 Relying party public key and certificate usage

Third parties relying on certificates issued by EADTrust must verify the validity of the certificates and are subject to the following obligations:

- Independently assess the appropriateness of the use of a certificate and determine that it will, in fact, be used for an appropriate purpose.
- Be aware of the conditions for using certificates in accordance with the provisions of the Certification Practice Statement, and especially in the PDS (Policy Disclosure Statement), i.e., the abbreviated statement for relying third parties.
- Check the validity or revocation of issued certificates, using the certificate status information available in the OCSP service.
- Check all certificates in the certificate hierarchy before trusting a digital signature or any of the certificates in the hierarchy. For qualified certificates, check that the EADTrust root certificate authority in whose hierarchy the certificate is located is included in the corresponding TSL list.
- Take into account the limitations of use of the certificates, whether they are contained in the certificate itself, in the PDS or, if applicable, in the verifier contract.
- Take into account the precautions included in a contract or other instrument, regardless of its legal nature.
- Notify EADTrust of any inaccuracies or defects in a certificate that may be considered grounds for revocation.
- Refrain from monitoring, interfering or reverse engineering the technical implementation of certification services without the prior written approval of the Certification Authority.
- Refrain from intentionally compromising the security of certification services.
- Assume that qualified electronic signatures are equivalent to handwritten signatures, in accordance with Article 25.2 of EU Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014.

4.6 Certificate renewal

Certificate renewal requests are treated as applications for new certificates.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

Certificate re-key requests are treated as applications for new certificates.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

Certificate modification requests are treated as applications for new certificates.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

Revocation shall be understood as a change in the status of a certificate due to the loss of validity of the certificate due to circumstances other than its expiration.

4.9.1 Circumstances for revocation

The circumstances to be taken into account for the revocation of certificates are the following:

- The revocation request has been made by the signatory, the natural or legal person represented by the signatory, an authorized third party or a natural person who applied for a digital certificate for a legal person.
- The signature creation data of the signatory or the certification service provider has been compromised or if the signatory or a third party has used the data incorrectly.
- When a legal or administrative order has been issued to that effect.
- The death of the signatory or the extinction of the legal entity holding the seal certificate, the unforeseeable total or partial incapacity of the signatory or the legal entity represented by the signatory, the termination of the representation, the dissolution of the represented legal entity, the change in the circumstances of the custody or use of the signature creation or seal data included in the certificates issued to a legal entity.
- The event that EADTrust terminates its activity, except in cases where the signatory has given consent for the electronic certificate management services to be transferred to another certification service provider.
- Change in the data provided to obtain the certificate or modification of the circumstances verified for the issuance of the certificate.

- The private key associated with the certificate has been lost, stolen or is no longer useful due to damage to the certificate support or when it has been changed to another support not foreseen in the certification policy.
- One of the parties fails to fulfill its obligations, such as, for example, payment.
- An error is detected in the certificate issuance procedure, either because one of the prerequisites has not been met or due to technical problems during the certificate issuance process.
- There is a potential threat to the security of the systems and to the reliability of certificates issued by EADTrust for reasons other than the compromise of signature creation data.
- Technical failure in the issuance or distribution of certificates or associated documentation.
- If EADTrust receives a request for certificate issuance and a valid certificate of the same class and uniqueness already exists, the valid certificate will be revoked at the request of the requestor.

Timeframes for revoking certificates under above reasons will be consistent with the timeframes required by "Baseline Requirements for Reasons for Revoking CA Certificate".

4.9.2 Who can request revocation

The revocation of a certificate may be requested by:

- The Subject/Signatory.
- The responsible Applicant.
- The Entity (through a representative).
- The RA or the CA.
- It can be done ex officio if EADTrust has evidence through other means that circumstances have arisen that make revocation necessary.
- In the case of bids, the request for revocation may be made by the persons designated by the contracting authority in compliance with the bid documents.

4.9.3 Procedure for revocation request

The Subscriber may contact EADTrust and request the revocation of a certificate. EADTrust will inform the Subscriber on how to formalize the request.

The certificate can be revoked at any time and must be revoked in all cases of loss or theft.

The authenticated revocation request and the information justifying the revocation is recorded and archived.

If the revocation is requested by someone other than the requestor, subscriber or key holder, prior to or concurrently with the revocation, EADTrust will inform the certificate key owner and the subscriber of the revocation of their certificate and specify the reason for revocation. The applicant may request revocation of the certificate through the following channels:

1. Online, by completing the revocation request form available at the address: www.eadtrust.eu.
2. By e-mail with an electronically signed request using a qualified certificate.

3. By postal mail addressed to EADTrust's address, sending the certificate revocation request signed and validated by a notary.
4. By a qualified certified delivery system that proves the identity of the sender, which must match with one of the parties entitled to request the revocation.

Subsequently, the applicant will be instructed to schedule an appointment with the EADTrust Registration Authority to verify the identity of the revocation applicant. This process will be conducted via video conference or qualified electronic signature.

Once it has been verified that the revocation request meets the requirements defined in this CPS, the certificate will be revoked.

In the case of bids, the conditions established by the contracting authority will be taken into account.

EADTrust maintains a continuous (24x7) ability to accept and respond to revocation requests and Certificate Problem Reports. EADTrust will respond to such requests within 24 hours, though an investigation into the legitimacy of the request may take longer.

An investigation into whether revocation or other appropriate action is warranted will be based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint; and
4. Relevant legislation.

4.9.4 Revocation request grace period

Once the revocation has been duly processed by the RA, the revocation information will be available through the OCSP service.

The caution period or grace period to be applied for the validation of certificates is the maximum time elapsed between CRL renewals (when this procedure is applied to check if a certificate is revoked).

The recommended grace period is 24 hours.

EADTrust maintains, in the CRLs, information on revoked certificates until the expiration date. However, it will keep available, beyond the expiration date, a repository of previous CRLs that will allow checking if a certificate was revoked before its expiration date with that historical information. This repository will maintain CRLs up to 1900 days old.

4.9.5 Time within which CA must process the revocation request

For end-entity certificates. The revocation period since EADTrust or an RA has authenticated knowledge of the revocation of a certificate, this occurs immediately, at most 10 minutes after the end of the communication that gives news of the reasons for the revocation, being incorporated in the next CRL to be issued and in the database of the management platform that consults the OCSP responder.

4.9.6 Revocation checking requirement for relying parties

Checking the status of certificates is mandatory for each use of the certificate, either by consulting the OCSP service or the Certificate Revocation List (CRL).

EADTrust provides information to verifiers on how and where to find the corresponding CRLs and OCSP service, in particular in the AIA (Authority Information Access) field of the certificate and in the "CRL Distribution Point" field.

4.9.7 CRL issuance frequency (if applicable)

EADTrust immediately issues a Certificate Revocation List (CRL) when a certificate is revoked.

The CRL contains the stipulated time for the issuance of a new CRL, although a CRL can be issued earlier than the time indicated in the previous one. If there are no revocations, the certificate revocation list is regenerated daily.

The CRL for end-entity certificates is issued every 24 hours or no later than 10 minutes after a revocation is confirmed. The CRL for CA certificates (ARL) is issued every 12 months or when a revocation occurs.

Revoked certificates that expire are not maintained in the CRL. However, a CRL is issued every day and maintained in a repository for up to 1900 days. In addition, all expired certificates (revoked or not) are retained in the EADTrust internal registry for a total period of 10 additional years from the expiration date.

No "Last CRLs" are generated. If a CRL expires and another CRL has not been issued within the stipulated period (date in the NextUpdate field), no subsequent CRLs will be issued. In case a CA is revoked, all certificates will be revoked and a CRL with all revoked certificates will be issued.

4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency time is set at 10 minutes.

4.9.9 On-line revocation/status checking availability

Revocation information for all certificates is made available via OCSP. OCSP responses are available at all times (24x7x365) if possible.

4.9.10 On-line revocation checking requirements

See Section 4.9.6.

4.9.11 Other forms of revocation advertisements available

EADTrust allows for OCSP stapling.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

EADTrust does not suspend certificates.

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

EADTrust provides User Entities with a real-time certificate checking service based on OCSP (Online CertificateStatusProtocol).

This service is available 24 hours a day, 7 days a week. As required by Regulation (EU) 910/2014 eIDAS, this service is provided free of charge.

4.10.2 Service availability

All certificate status services are made available at all times (24x7x365) if possible.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

A Subscriber's subscription ends once all of Subscriber's EADTrust certificates have expired or been revoked.

Prior to expiration of a Subscriber's certificate, EADTrust may send Subscriber a notice regarding upcoming Certificate expiration if a contact email address was provided.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

EADTrust has adequate infrastructure to provide digital trust services in its facilities in Madrid, and also for certain services (OCSP, for example) may be contracted Hosting and Cloud Computing Service Providers, such as Amazon and OVH.

5.1.2 Physical access

Physical access to EADTrust Secure PKI Facilities is restricted to authorized EADTrust employees, vendors, and contractors, for whom access is required in order to execute their jobs. Access restrictions are strongly enforced via multi-factor authentication mechanisms.

5.1.3 Power and air conditioning

The Secure PKI Facilities has sufficient power and air conditioning to create a reliable operating environment.

The service equipment has low power consumption and low heat dissipation so that it can continue in use even if the air conditioning fails for an extended period of time.

The uninterruptible power supply systems guarantee an operating time of more than 10 hours in the event of a prolonged power failure.

In the event of an extended power outage, systems will be shut down in an orderly manner. OCSP systems that report certificate revocation status are not affected by system downtime as they can be managed in an externally hosted high availability environment.

5.1.4 Water exposures

EADTrust Secure PKI Facilities are designed to protect EADTrust infrastructure from water exposure/damage. Its facilities are located in a geographically elevated location.

5.1.5 Fire prevention and protection

EADTrust Secure PKI Facilities are designed to prevent fire and provide suppression if necessary. It has physical barriers that extend from the floor to the ceiling, as well as automatic humidity and temperature measurement systems that will register abnormal situations before a fire can break out.

It has extinguishing equipment that is properly marked and appropriate to the type of equipment in place. The door has additional fireproof foam protection.

5.1.6 Media storage

EADTrust Secure PKI Facilities are designed to prevent accidental damage or unauthorized access to media.

5.1.7 Waste disposal

There is a policy to regulate the procedures governing the destruction of information media.

Storage media containing confidential information are destroyed to ensure that the data is not readable or recoverable after disposal. EADTrust has adopted a waste management policy designed to pass an ISO 14001 audit.

5.1.8 Off-site backup

EADTrust maintains a system of encrypted backups of certain keys in a secure on-site repository.

In addition, encrypted backups of systems, databases and source code are maintained in a cloud repository.

5.2 Procedural controls

5.2.1 Trusted roles

A "Trusted Role" is defined as duties assigned to an individual that can lead to safety concerns if not performed satisfactorily, either accidentally or intentionally.

To ensure that trusted roles properly perform their duties, the following considerations are addressed:

- The first is that the technology is designed and configured to prevent errors and inappropriate behavior.

- The second is that the tasks are distributed among several individuals so that any misconduct would require the complicity of several individuals.

EADTrust has complete definitions of all the functions performed in the organization. The duties and responsibilities associated with each function are defined, and each has a set of documented procedures governing the practice attached to each.

Trusted Roles include:

- Security Officers: Overall responsibility for administering the implementation of the security practices.
- System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.
- System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.
- System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.

5.2.2 Number of persons required per task

To reinforce the security of the system, more than one person is assigned to each function, with the exception of the operator function, which can be performed by the administrator.

Several people can be assigned to the same function.

5.2.3 Identification and authentication for each role

Trusted Roles require identity verification by secure means before accessing EADTrust PKI systems or confidential information. All Trusted Roles are performed by individuals.

EADTrust has specific documentation that gives more details of each role.

5.2.4 Roles requiring separation of duties

EADTrust follows the CIMC (Certificate Issuing and Management Component) security policy defined in its security model.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

EADTrust management is responsible for making sure that Personnel with Trust functions are trustworthy and competent, which includes having proper qualifications and experience.

EADTrust management ensures this with appropriate interviewing practices, training, background checks, and regular monitoring and review of Trusted Contributor job performance.

5.3.2 Background check procedures

According to Spanish law, it is not applicable for companies to request a criminal record from employees. There is a general prohibition to discriminate against any worker, for any reason, both in employment and in access to employment. This is specifically regulated in Article 14 of the Spanish Constitution, Article 4.2 of the Workers' Statute and Article 73.2 of the General Penitentiary Law.

In accordance with Spanish legislation and the reiterated criteria of the courts, the right to privacy and labour reinsertion must take precedence.

In any case, probity checks are carried out.

5.3.3 Training requirements

Trusted Contributors must be trained on topics relevant to the role in which they will perform.

Training programs are developed for each role by EADTrust management and Security Officers. And they include the following:

- A copy of the Trusted e-Services Statement of Practice.

- Security awareness.

- Software and hardware operation for each specific function.

- Security procedures for each specific function.

- Management and operating procedures for each specific function.

- Disaster recovery procedure.

- Incident management procedure

Among the applicable security requirements are those included in the Information Security Management System developed within the framework of ISO 27001 certification.

5.3.4 Retraining frequency and requirements

Any significant changes to EADTrust PKI operations will require a training plan and the implementation of the plan will be documented.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Action will be taken to safeguard EADTrust and its subscribers whenever EADTrust Trusted Contributors, whether through negligence or malicious intent, fail to comply with EADTrust policies including this CPS.

Actions taken in response to non-compliance may include termination, removal from trusted roles, or reporting to legal authorities.

Information security incidents. EADTrust has a security incident management procedure designed taking into consideration the technical guidelines defined by the European Union Agency for Network and Information Security ENISA in the document; "Article 19 Incident reporting. (Incident reporting framework for eIDAS Article 19).”

Sanctions for unauthorized actions. EADTrust applies the disciplinary system and sanctions defined in the labour current legislation, taking into consideration the circumstances of the facts, the persons involved, and the seriousness of the actions.

5.3.7 Personnel hiring requirements

EADTrust maintains a recruitment policy that seeks the appropriate profiles for its activity and has suitability criteria for the assignment of roles and responsibilities.

EADTrust complies with its obligations in terms of equality and, within the framework of its relations with its employees, has assumed a reliable commitment to the promotion and effective implementation of the principles of equal opportunities between women and men, and non-discrimination on the basis of gender, race, origin, religion, etc.

In the same sense, it expresses its commitment to work to ensure the accessibility of its services and facilities to all people, regardless of their technical, cognitive or physical abilities.

5.3.8 Independent Contractor Controls

Independent contractors who are assigned to perform Trusted Roles are subject to the duties and requirements specified for such roles in this CPS and the EADTrust CP. This includes those described in Section 5.3. Potential sanctions for unauthorized activities by independent contractors are described in Section 5.3.6.

5.3.9 Documentation supplied to personnel

All personnel in positions of trust are provided with all documentation necessary to perform their duties. This always includes, at minimum, a copy of the EADTrust CP, a copy of the CPS, a copy of the Welcome Manual that includes specific confidentiality and security considerations, the documentation defining the duties and procedures associated with each role, and they will also have access to the operations manuals of the different components of the system.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Audit logs are generated for all events related to CA security (physical and logical) and certificate issuance. Logs are automatically generated whenever possible. When it is necessary to manually log information, logs are kept on paper with written confirmation from a witness and securely stored. All audit logs, electronic or otherwise, shall be retained and made available to compliance auditors upon request.

At a minimum, each audit record includes:

- Date and time of entry;
- Identity of the person (or machine) making the entry; and
- Description of the entry.

5.4.2 Frequency of processing log

Audit records are reviewed regularly by EADTrust's internal auditor.

5.4.3 Retention period for audit log

Audit logs are retained for at least ten years and will be made available to compliance auditors upon request.

5.4.4 Protection of audit log

Audit logs, whether in production or archived, are protected using both physical and logical access controls.

5.4.5 Audit log backup procedures

The backup management systems are included among the security measures adopted by the entity.

When there is any CA management, a backup copy of the previous situation is made and the action is also recorded in the log.

5.4.6 Audit collection system (internal vs. external)

Audit data is automatically generated and reported/recorded by operating systems, CA software applications, and network devices. Systems are in place to ensure proper reporting and recording of audit data, and the failure of such systems may lead to suspension of CA services until proper audit log reporting is restored.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Vulnerability analysis is covered by EADTrust audit processes.

Risk and vulnerability management processes are reviewed annually within the framework of the UNE-ISO/IEC 27001 certification review, which are reflected in the EADTrust Risk Analysis document.

This document specifies the controls implemented to guarantee the required security objectives.

In addition, "White Hat Ethical Hacking" or "Penetration Testing" audits are contracted externally.

Quarterly, internal auditors perform additional "Penetration Testing" procedures

5.5 Records archival

5.5.1 Types of records archived

EADTrust archives all audit logs, the contents of which are described in Section 5.4.1. EADTrust may also archive any other information deemed critical to understanding the historical performance of the CA's duties.

5.5.2 Retention period for archive

EADTrust retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least fifteen years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of archive

Archives are protected from unauthorized modification or destruction by strong security and environmental controls at primary and offsite storage facilities.

5.5.4 Archive backup procedures

Archives are backed up at primary CA facilities.

5.5.5 Requirements for time-stamping of records

Records are time-stamped as they are created.

Machine-created records use system time, which is synchronized automatically with third-party time sources. Machines without network access have the time set manually.

Manual records use a manually entered date and time, complete with time zone in use.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

There is no specific provision for key changes.

Each time a CA or Sub CA is generated, it is carried out within the framework of a ceremony of which a record is kept and in which private and public keys are established, leaving the public keys contained in the certificate associated with the generation, with the data corresponding to the type of CA.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

EADTrust has created and maintains incident response procedures for a range of potential compromise and disaster situations. Such situations include, but are not limited to, natural disasters, security incidents, and equipment failure. Incident response plans are reviewed, potentially updated, and tested on at least an annual basis.

5.7.2 Computing resources, software, and/or data are corrupted

In the event that computing resources, software, and/or data are corrupted or otherwise damaged, EADTrust will assess the situation, including its impact on CA integrity and security, and take appropriate action. CA operations may be suspended until mitigation is complete. Subscribers may be notified if corruption or damage has a material impact on the service provided to them.

5.7.3 Entity private key compromise procedures

In the event that a CA Private Key is compromised, or suspected to be compromised, EADTrust will immediately launch a thorough investigation. Forensic evidence will be collected and secured as quickly as possible. If it cannot be determined with a high degree of certainty that the private key in question was not compromised, then the following steps may be taken in whatever order is deemed most appropriate by EADTrust Security Officers:

- Certificates relying on the private key in question will be revoked.
- EADTrust will notify root programs relying on the integrity of the key in question.
- EADTrust will notify Subscribers relying on the integrity of the key in question.

5.7.4 Business continuity capabilities after a disaster

EADTrust maintains offline backup copies of the root CA on two different locations. In the event that a disaster entirely disables one facility, EADTrust CA operations will fail over to another facility.

5.8 CA or RA termination

In the event that EADTrust CA services are to be terminated:

- All affected parties, including root programs and Subscribers, will be provided with notice at least two months prior to the termination of the operations.
- A termination plan will be created and review by the EADTrust PMA.

If a suitable successor entity exists, the following steps will be taken:

- CA Private Keys, records, logs, and other critical documentation will be transferred to the successor organization in a secure and compliant manner.
- Arrangements will be made for compliant continuation of CA responsibilities.

If a suitable successor entity does not exist, the following steps will be taken:

- All certificates issued will be revoked and final CRLs will be published.
- CA Private Keys will be destroyed.
- CA records, logs, and other critical documentation will be transferred to a third party or government entity with appropriate legal controls in place to protect information while allowing its use in compliance with relevant policies and the law.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

EADTrust's own key management systems as a Digital Trust Service Provider in its certification hierarchies use specific software and devices for the protection of private keys.

Root CAs are managed through off-line procedures, while subordinate CAs are managed on qualified signature creation devices that allow on-line operation with rigorous operational controls.

Prior to the expiration of a CA certificate, EADTrust will perform, well in advance, at least one (1) month, a new key generation ceremony for the CA concerned by this situation.

No Sub CA certificates will be issued with an expiration date later than that of the issuing CA.

End-entity certificates shall not be issued with an expiration date later than that of the issuing CA.

Root and Sub CA certificates shall be available in the EADTrust web-accessible repositories, even when they have expired.

6.1.2 Private key delivery to subscriber

Certificates issued in a software mechanism with private key generation. In this case an encrypted PKCS#12 file is delivered with a different decryption key delivery mechanism, reinforced with channel diversity. The private key is removed when the PKCS#12 file is generated and the PKCS#12 file is removed when the download is confirmed by the client.

6.1.3 Public key delivery to certificate issuer

The method used to deliver the public key to the EADTrust RA is as follows:

- Issuing CAs: the public key is sent to the root issuing entity in X.509 or PKCS#10 format (this is the case for certificate request).
- Software certificate mechanism: the public key is sent to the EADTrust CA in PKCS#10 format.

6.1.4 CA public key delivery to relying parties

EADTrust CA public keys are available through the EADTrust website.

6.1.5 Key sizes

The hashing algorithm used is SHA-2 or later. The use of SHA-1 algorithm is excluded.

The root authority key size, depending on each case, is:

- Regarding the RSA algorithm: key sizes of 2048 bits, 4096 and 8192.
- Regarding the ECC algorithm: ECDSA 256 (prime256v1) and ECDSA 384 (secp384r1).

6.1.6 Public key parameters generation and quality checking

Key generation has been verified so that it is not susceptible to a ROCA (Return of Coppersmith Attack) attack.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

See Section 7, Certificate Profiles.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

EADTrust uses HSMs meeting FIPS 140-2 Level 3 (or higher) requirements.

6.2.2 Private key (n out of m) multi-person control

The use of CA private keys requires at least two people. On the one hand, access control to the devices, and on the other hand, knowledge of the keys and access to the computer processes that allow the generation of keys and certificates.

6.2.3 Private key escrow

There is a security management procedure that allows reconstructing the private key of the root key encryption mechanism by accessing a Notary that holds a fraction of the key, but also requires another fraction held in EADTrust's physical security systems.

6.2.4 Private key backup

There is a procedure for the recovery of keys to the cryptographic module of the subordinate CAs that can be applied in case of contingency. The same multi-person controls as indicated above will be applied.

6.2.5 Private key archival

EADTrust does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

EADTrust CA Private Keys are generated inside HSMs and are only transferred between HSMs for redundancy or backup purposes. When transferred, keys are encrypted prior to leaving HSMs and unwrapped only inside destination HSMs. Keys never exist in plain text form outside of HSMs.

6.2.7 Private key storage on cryptographic module

There is a CA key procedure document that describes the processes for generating the private key and the use of cryptographic hardware.

In generating CA keys, EADTrust follows the recommendations of ETSI EN 319 411 and the Basic Requirements Guidelines 17.7.

In cases where private keys are stored outside the cryptographic modules, they shall be protected to ensure the same level of protection as if they were physically inside the cryptographic modules. All HSMs used by EADTrust to store private keys for Certification Authorities have FIPS 140-2 level 3 certification, or Common Criteria EAL4+.

6.2.8 Method of activating private key

The root CA and the keys of the subordinate CAs are activated by a process that requires at least dual control for access and management of the cryptographic devices (cryptographic tokens or cards).

The subscriber/certificate holder accesses the private key via a PIN. The device has a system that protects it against access attempts that block it when the wrong code is entered a certain number of times. The subscriber/certificate holder has a device unlock code. If it is entered incorrectly a certain number of times, the device is permanently locked and the information contained inside it cannot be retrieved.

6.2.9 Method of deactivating private key

The deactivation of the private key will be carried out with the revocation of the certificate associated to the public key corresponding to the deactivated private key.

6.2.10 Method of destroying private key

There is a procedure for the destruction of CA keys.

In case of removal of the HSM containing the CA keys, they will be destroyed. The HSM itself includes a motion detection system that initializes the device.

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

See Section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The period in which the private key associated with the public key included in the certificates can be used must be between the date of issuance of the certificate and the expiration date.

The validity period of the certificates issued by EADTrust can be verified by consulting the information contained in the certificate field named: validity.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data used to activate CA Private Keys is generated during a key ceremony. Activation data is transferred to the person who will use it, or place it will be stored, in a secure fashion.

6.4.2 Activation data protection

Activation data is protected from unauthorized disclosure via a combination of physical and logical means.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

EADTrust CA infrastructure and systems are appropriately secured in order to protect CA software and data from unauthorized access or modification. Access to systems is secured via multi-factor authentication whenever possible. Security updates are applied in a timely fashion. Vulnerability scans are run regularly.

6.5.2 Computer security rating

The products used for the provision of certification services have the international qualification of "Common Criteria" or ISO Standard, ISO/IEC 15408. Failing that, they can be certified based on the FIPS-140-2 standard.

6.6 Life cycle technical controls

6.6.1 System development controls

There is a repository for software version control.

Production systems are periodically reviewed to check that security updates released by developers are correctly applied. In particular: operating system, databases and critical applications.

In-house developments are checked before they go into production.

To avoid potential problems with these systems, the following controls are applied:

- There are coordination practices for updating software libraries (including patches) in production. Approval is granted only after ensuring that it is working properly.
- The test system is kept separate from the production system to ensure that it is working properly before moving to production.
- A dependency registry is in place to ensure that an upgrade does not disable a required security feature so that the appropriate version level can be controlled.
- Previous versions of proprietary software are retained.
- Purchased software is maintained at the level supported by the vendor unless there are identified dependencies that require an earlier version.

6.6.2 Security management controls

EADTrust conducts internal and external audits to verify the correct application of its policies. These include:

- ISO 27001 audit
- Ethical hacking audits (penetration tests)
- eIDAS standard audit
- Other security audits (ENS Esquema Nacional de Seguridad, Spanish Audit Scheme)

6.6.3 Life cycle security controls

EADTrust services involving a trusted relationship with customers and users will involve the lifecycle management of the relationship. The certificate issuance lifecycle is one of those covered by this relationship.

The security controls applied in the life cycle of the certificates have a particular impact on the request for certificates and their revocation.

6.7 Network security controls

Monitoring systems are in place in EADTrust's internal network to record incidents, including those affecting security, and to notify operators of the need for action.

Firewalls are reviewed when filtering rules need to be updated.

All security measures and controls specified for the rest of the systems are applied to network devices and are set out in the Security Policy.

Users can only access services for which they are authorized.

6.8 Time-stamping

See Section 5.5.5.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All fields are as specified in RFC5280, including fields and extensions not specifically mentioned. Extensions are not marked critical unless specifically described here as critical.

Qualified Web Site Certificate “Domain Validated” or “Organization validation”

Field/Extension	Critical	Value
Version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
Signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
Issuer		Same as the Subject field of the issuing CA certificate

Field/Extension	Critical	Value
Validity		379 days
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41241
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.194112.1.5 (ETSI QNCP-w)
policyIdentifier		2.23.140.1.2.1 (CAB/FORUM DV) or *2.23.140.1.2.2 (CAB/FORUM OV)*
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eaddvov<Year>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eaddvov<Year>.crt
Ocsp		http://ocsp.eadtrust.eu
basicConstraint	Critical	CA false
qcStatements		
QcRetentionPeriod		15 years
QcCompliance		Present
QcType		id-etsi-qct-web
keyUsage	Critical	digitalSignature
CT RFC6962		Certificate Transparency

This type of certificate is issued under the qualified web hierarchies of domain validation and organization validation and supports different variants.

EIDAS Policy QNCP-w (certificate policy for EU qualified website authentication certificates based on NCP and PTC) as defined by CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates". OID: `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qncp-web (5)`

Qualified Web Site Certificate “PSD2” (QWAC)

Field/Extension	Critical	Value
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate

Field/Extension	Critical	Value
validity		379 days
subject		
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
serialNumber		Registration Number
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41243
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eadevpsd2<Year>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eadevpsd2<Year>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Critical	CA false
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15 years
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
PSD2QcType		ETSI TS 119 495 Format
keyUsage	Critical	digitalSignature
CT RFC6962		Certificate Transparency
cabfOrganizationIdentifier		Effective January 31, 2020, if the subject:organizationIdentifier field is present, this field MUST be present

This type of certificates is issued under the Qualified Web Hierarchies (QWAC) of Extended validation and PSD2 (QWAC) and supports different variants.

Qualified Web Site Certificate "Extended Validation" (QWAC)

Field/Extension	Critical	Value
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
serialNumber		Registration Number
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41244
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eadevpsd2<Year>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eadevpsd2<Year>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Critical	CA false
qcStatements		
QcCompliance		Present
QcType		id-etsi-qct-web
QcRetentiodPeriod		15 years

Field/Extension	Critical	Value
keyUsage	Critical	digitalSignature
CT RFC6962		Certificate Transparency

This type of certificate is issued under the qualified web hierarchies (QWAC) of Extended validation and PSD2 and supports different variants.

EIDAS Policy QEVCP-w (certificate policy for EU qualified website authentication certificates based on EVCP). OID: `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)`

Qualified Web Site Certificate for e-Office "Extended Validation" (QWAC) - High Assurance Level

Field/Extension	Critical	Value
version		3
serialNumber		positive integer, not larger than 20 bytes *
signature		SHA-2 with RSA.
issuer		Same Subject as the issuer´s certificate. Fields Country Common Name Organization
validity		372 days
subject		
OrganizationalUnit		OU= "SEDE ELECTRONICA"
OrganizationalUnit		The descriptive name of the office. OU= e.g.: GENERAL ACCES POINT
businessCategory		businessCategory = "Government Entity"
jurisdictionCountryName		jurisdictionCountryName= "ES"
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Denomination ("official" name of the organization) of the certificate services subscriber (certificate custodian)
Common Name		Domain name system (DNS) where the certificate Will reside. CN= e.g. administración.gob.es
LocalityName		City
StateOrProvinceName		State or province name
CountryName		State whose law governs the name, which will be ES ("Spain") because they are public entities.
serialNumber		The tax ID number of the responsable entity. SerialNumber = e.g.: S2833002. Size [RFC 5280] 64
Organization Identifier		Organization identifier. According to the technical standard ETSI EN 319 412-1 (VATES + tax ID number of the organization) OrganizationIdentifier e.g.: VATES-S2833002.
subjectPublicKeyInfo		RSA 2048 bits
Extensions		
subjectAltName		

Field/Extension	Critical	Value
dnsName		DNS name(s)
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Public key identifier of the subscriber's or key holder's public key (derived by using the Hash function on the public key of the subject). Means of identifying certificates that contain a particular public key and facilitates the construction of certification routes.
authorityKeyIdentifier		Means to identify the public key corresponding to the private key used to sign a certificate, for example, in cases where the issuer has multiple signing keys.
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41246
cpsURI		http://policy.eadtrust.eu
userNotice		E.g.: "Qualified e-Office certificate, high level. See conditions of use in " + URLof the CPS or, if applicable, third party legal document.
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
policyIdentifier		2.16.724.1.3.5.5.1
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keysize >eadevpsd2<Year>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keysize >eadevpsd2<Year>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Critical	CA false
qcStatements		
QcCompliance		Indication of qualified certificate
QcType		id-etsi-qct-web
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describes the retention period of all information relevant to the use of a certificate after its expiration) OID 0.4.0.1862.1.3
QcPDS		Location of the PDS statement
semanticsId-Legal		To indicate legal entity semantics as defined by EN 319 412-1
keyUsage	Critical	digitalSignature
CT RFC6962		Certificate Transparency (when we are in CA/B Forum)
cabfOrganizationIdentifier		(OID: 2.23.140.3.1) If the subject:organizationIdentifier is present, this field MUST be present.

EV certificates may be multi-domain but CANNOT be issued with wildcard subdomain qualifiers.

Non-qualified Web Site Certificate "Domain Validated"

Field/Extension	Critical	Value
Version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
Signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384

Field/Extension	Critical	Value
Issuer		Same as the Subject field of the issuing CA certificate
Validity		379 days
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41247
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.2042.1.6 (ETSI DVCP)
policyIdentifier		2.23.140.1.2.1 (CAB/FORUM DV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eaddvov<Year>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eaddvov<Year>.crt
Ocsp		http://ocsp.eadtrust.eu
basicConstraint	Critical	CA false
keyUsage	Critical	digitalSignature
CT RFC6962		Certificate Transparency

This type of certificate is issued under the qualified web hierarchies (QWAC) of domain validation and organization validation and can be issued in several different variants

Non-qualified Web Site Certificate “Organization Validated”

Field/Extension	Critical	Value
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		
subjectAltName		
dnsName		DNS name(s)

Field/Extension	Critical	Value
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41248
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.2042.1.7 (ETSI OVCP)
policyIdentifier		2.23.140.1.2.2 (CAB/FORUM OV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eaddvov<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eaddvov<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Critical	CA false
keyUsage	Critical	digitalSignature
CT RFC6962		Certificate Transparency

This type of certificate is issued under the qualified web hierarchies (QWAC) of domain validation and organization validation and supports different variants.

Non-qualified Web Site Certificate "Extended Validation"

Field/Extension	Critical	Value
version		3
serialNumber		Unique non-sequential positive number of minimum length 64 bits
signature		Sha256WithRSAEncryption or ecdsa-with-SHA256 or ecdsa-with-SHA384
issuer		Same as the Subject field of the issuing CA certificate
validity		379 days
subject		
businessCategory		Private Organization, Government Entity, Business Entity or Non-Commercial Entity
jurisdictionCountryName		Country of Jurisdiction of Incorporation or Registration Field
jurisdictionStOrProvName		State or Province of Jurisdiction of Incorporation or Registration Field
jurisdictionLocalityName		Locality of Jurisdiction of Incorporation or Registration Field
OrganizationName		Organization Name
LocalityName		Locality Name
StateOrProvinceName		State or province name
CountryName		CountryName
serialNumber		Registration Number
OrganizationIdentifier		ETSI EN 319 412-1 and CA/B Forum format
subjectPublicKeyInfo		RSA 2048 bits minimum or ECDSA 256 bits (prime256v1) or 384 bits (secpr384r1)
Extensions		

Field/Extension	Critical	Value
subjectAltName		
dnsName		DNS name(s)
extendedKeyUsage		serverAuth, clientAuth
subjectKeyIdentifier		Derived from the result of applying the hash to the public key of the subject
authorityKeyIdentifier		Derived from the result of applying the hash to the public key of the issuing CA
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41249
cpsURI		http://policy.eadtrust.eu
policyIdentifier		0.4.0.2042.1.4 (ETSI EVCP)
policyIdentifier		2.23.140.1.1 (CAB/FORUM EV)
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eadevpsd2<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algorithm><keysize>eadevpsd2<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Critical	CA false
keyUsage	Critical	digitalSignature
CT RFC6962		Certificate Transparency
cabfOrganizationIdentifier		Effective January 31, 2020, if the subject:organizationIdentifier field is present, this field MUST be present

This type of certificate is issued under the qualified web hierarchies (QWAC) of Extended validation and PSD2 (QWAC) and supports different variants.

7.1.1 Version number(s)

All certificates use X.509 version 3.

7.1.2 Certificate extensions

See section 7.1.

7.1.3 Algorithm object identifiers

Name	Object identifier
Qualified Web Site Certificate “Domain Validated” (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41241
Qualified Web Site Certificate “Organization Validation” (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41242
Qualified Web Site Certificate “PSD2” (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41243
Qualified Web Site Certificate “Extended Validation” (QWAC)	1.3.6.1.4.1.501.2.1.1.0.41244

Name	Object identifier
Qualified Web Site Certificate for e-Office "Extended Validation" (QWAC) - High Assurance Level	1.3.6.1.4.1.501.2.1.1.0.41246
Non-qualified Web Site Certificate "Domain Validated"	1.3.6.1.4.1.501.2.1.1.0.41247
Non-qualified Web Site Certificate "Organization Validated"	1.3.6.1.4.1.501.2.1.1.0.41248
Non-qualified Web Site Certificate "Extended Validation"	1.3.6.1.4.1.501.2.1.1.0.41249

7.1.4 Name forms

See EADTrust Certificate Policy.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

See section 7.1.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

See section 7.1.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

CRL's issued by EADTrust are issued in accordance with the following standards:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile - April 2002.
- RFC 4325: Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension - December 2005.
- RFC 4630: Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile -August 2006.

7.2.1 Version number(s)

See section 7.2.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

EADTrust OCSP responders implement the RFC 5019 profile of RFC 6960.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

eIDAS compliance audits are intended to ensure a CA's compliance with its CP and CPS and relevant eIDAS audit criteria.

8.1 Frequency or circumstances of assessment

eIDAS compliance audit periods cover no more than one year and are scheduled by EADTrust annually, every year with no gaps.

See Section 8.7 for information about the frequency of self-audits.

8.2 Identity/qualifications of assessor

EADTrust's eIDAS compliance audits are performed by a qualified auditor. A qualified auditor means a natural person, legal entity, or group of natural persons or legal entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit (which is EADTrust);
2. The ability to conduct an audit that addresses the relevant criteria
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the eIDAS standard) licensed by eIDAS;
6. Bound by law, government regulation, or professional code of ethics; and

7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3 Assessor's relationship to assessed entity

EADTrust's eIDAS auditors shall have no financial interest in, or other type of relationship with, EADTrust, which might cause the auditors to have a bias for or against EADTrust.

8.4 Topics covered by assessment

Compliance audits cover EADTrust's compliance with the EADTrust CP and this CPS, as well as the following eIDAS principles and criteria:

- Principles and Criteria for Certification Authorities
- eIDAS Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

8.5 Actions taken as a result of deficiency

Noncompliance with relevant requirements will be documented by auditors (internal or external), the EADTrust PMA will be informed, and the EADTrust PMA will ensure that steps are taken to address the issues as quickly as reasonably possible.

8.6 Communication of results

Audit results are reported to the EADTrust PMA and any other entity entitled to the results by law, regulation, or agreement. This includes a number of Web user agent (i.e., browser) root programs.

EADTrust is not required to publicly disclose any audit finding that does not impact the overall audit opinion.

8.7 Self-Audits

EADTrust performs at least annual internal audit of at least 3% of issuance since the last eIDAS audit period. The sample is randomly selected. Results are saved and provided to auditors upon request.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees that users must pay in consideration for the service are included in the terms and conditions of issuance for each type of certificate.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

EADTrust does not charge any fees for certificate revocation or for checking the validity status of an issued certificate using a CRL or OSCP, according to European Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

EADTrust does not have an established refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

EADTrust has a Civil Liability Insurance appropriate to its activities, in accordance with the regulations governing electronic trust services.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

EADTrust employees, agents, and contractors are responsible for protecting confidential information and are bound by EADTrust's policies with respect to the treatment of confidential

information or are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4 Privacy of personal information

9.4.1 Privacy plan

EADTrust follows the privacy policy posted on its website (http://eadtrust.rgpd.de/en/privacy-policy/) when handling personal information.

9.4.2 Information treated as private

The privacy policy posted on EADTrust's website (http://eadtrust.rgpd.de/en/privacy-policy/) identifies information that EADTrust treats as private.

9.4.3 Information not deemed private

The privacy policy posted on EADTrust's website (http://eadtrust.rgpd.de/en/privacy-policy/) identifies information that EADTrust does not treat as private.

9.4.4 Responsibility to protect private information

EADTrust employees and contractors are subject to policies or contractual obligations requiring them to comply with EADTrust's privacy policy (http://eadtrust.rgpd.de/en/privacy-policy/) or contractual obligations at least as protective of private information as EADTrust's privacy policy.

9.4.5 Notice and consent to use private information

EADTrust follows the privacy policy posted on its website (http://eadtrust.rgpd.de/en/privacy-policy/) when using personal information.

9.4.6 Disclosure pursuant to judicial or administrative process

EADTrust may disclose personal information if compelled to do so by court order or other compulsory legal process, provided that EADTrust will oppose such disclosure with all legal and technical tools reasonably available to EADTrust.

9.4.7 Other information disclosure circumstances

EADTrust may disclose personal information under other circumstances that are described in the privacy policy posted on its website (http://eadtrust.rgpd.de/en/privacy-policy/).

9.5 Intellectual property rights

EADTrust and/or its business partners own the intellectual property rights in EADTrust's services, including the certificates, trademarks used in providing the services, and this CPS. Certificate and revocation information are the property of EADTrust. EADTrust grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are

reproduced and distributed in full. Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

Notwithstanding the foregoing, third party software (including open-source software) used by EADTrust to provide its services is licensed, not owned, by EADTrust.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, EADTrust does not make any representations or warranties regarding its products or services. EADTrust represents and warrants, to the extent specified in this CPS, that:

1. EADTrust complies, in all material aspects, with the CP and this CPS,
2. EADTrust publishes and updates CRLs and OCSP responses on a regular basis,
3. All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the CAB Forum Baseline Requirements, and
4. EADTrust will maintain a repository of public information on its website.

9.6.2 RA representations and warranties

EADTrust does not use RA services from third parties.

9.6.3 Subscriber representations and warranties

EADTrust will require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and assurances in this section for the benefit of the CA and the Certificate Beneficiaries. Prior to the issuance of a Certificate, the CA shall obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber's Agreement with the CA, or.
2. The applicant's acknowledgement of the Terms of Use.

Both the Subscriber Agreement and the certificate's Terms of Use shall be legally enforceable against the certificate Applicant.

A separate Agreement may be used for each certificate application, or a single Agreement may be used to cover multiple future certificate applications and the resulting Certificates, provided that each Certificate issued to the Applicant is clearly covered by the Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use shall contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under an outsourcing or hosting service relationship) the following obligations and warranties:

1. Accuracy of Information: obligation and warranty to provide accurate and complete information at all times to the CA, both in the application for the Certificate and in any other form requested by the CA in connection with the issuance of the Certificate(s) to be provided by the CA;

2. Protection of the private key: Obligation and warranty of the applicant to take all reasonable steps to ensure the control, confidentiality and adequate protection at all times of the private key corresponding to the public key to be included in the Certificate(s) applied for (and any associated activation device or data, e.g., password or token); 3.
3. Acceptance of the Certificate: Obligation and assurance that the Subscriber will review and verify the accuracy of the Certificate's content;
4. Use of Certificate: Obligation and warranty to install the Certificate only on servers that can be accessed by the subjetAltName listed in the Certificate, and to use the Certificate only in accordance with all applicable laws and only in accordance with the Subscriber Agreement or the Terms of Use;
5. Reporting and Revocation: Obligation and Warranty to: (a) immediately request revocation of the Certificate and cease use of the Certificate and its associated Private Key if there is actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) immediately request revocation of the Certificate and cease use if there is information in the Certificate that is or becomes incorrect or inaccurate.
6. Termination of Certificate Use: Obligation and warranty to immediately discontinue use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of the Certificate for reasons of key compromise.
7. Responsiveness: Obligation to respond to instructions from the CA regarding Key Compromise or Certificate misuse within a specified period of time.
8. Acknowledgement and Acceptance: An acknowledgement and acceptance that the CA has the right to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activity, such as phishing attacks, fraud, or malware distribution.

9.6.4 Relying party representations and warranties

Each Relying Party represents and warrants that, prior to relying on an EADTrust certificate, it:

1. Obtained sufficient knowledge on the use of digital certificates and PKI,
2. Studied the applicable limitations on the usage of certificates and agrees to EADTrust's limitations on its liability related to the use of certificates,
3. Has read, understands, and agrees to this CPS,
4. Verified both the EADTrust certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use an EADTrust certificate if the certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on an EADTrust certificate after considering:

- Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
- The intended use of the certificate as listed in the certificate or this CPS,
- The data listed in the certificate,
- The economic value of the transaction or communication,

- The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
- The Relying Party's previous course of dealing with the Subscriber,
- The Relying Party's understanding of trade, including experience with computer-based methods of trade, and
- Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a certificate is at a party's own risk.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

In case of a complaint from the user or an interested third party, he/she may send his/her complaint to the following e-mail address: info@eadtrust.eu or by mail; providing a copy of his/her identification; as well as all the documents and all the information he/she deems appropriate to support his/her complaint.

The CA of EADTrust will send within 48 hours by the same means of communication used by the applicant, a substantiated response report.

The time limit defined above may be extended in the event that the resolution of the complaint is complex for its solution. This extension will be communicated to the user.

In case the user is not satisfied with the resolution of the complaint. The user may file a request for an appeal to the General Management of EADTrust. To do so, the user should only communicate via e-mail to info@eadtrust.eu, indicating in the subject line that it is an appeal, or by post.

For the resolution of appeals, the procedure described above will be followed.

Complaints addressed to EADTrust will be handled directly in an attempt to reach an agreement to resolve the incident or, if applicable, to verify if it is a coverage included in the insurance. The activity of EADTrust is governed by Spanish Law and by the Courts of Madrid, unless the user is a consumer, which will result in the application of consumer protection regulations.

9.8 Limitations of liability

EADTrust shall not be liable for any damages arising out of or in connection with the non-performance or defective performance of a Certificate Holder's obligations.

EADTrust shall not be liable for the misuse of Certificates or keys, or for any consequential damages that may result from the use of Certificates.

EADTrust shall not be liable for any damages arising from transactions where the limitations on use of the Certificate have been breached.

EADTrust shall not be liable for any failure to perform or delay in performing any of the obligations contained in this Policy if such failure or delay is the result of force majeure, acts of God or, in general, any circumstance over which it has no direct control.

EADTrust shall not be responsible for the content of those documents electronically signed by certificate holders.

EADTrust does not guarantee the cryptographic algorithms and will not be liable for damages caused by successful external attacks on the cryptographic algorithms used, if due diligence was performed according to the current state of the art, and proceeded in accordance with the provisions of this Policy and the applicable regulations.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

Each Subscriber will indemnify and hold harmless EADTrust and its directors, officers, employees, agents, and affiliates from any and all liabilities, claims, demands, damages, losses, costs, and expenses, including attorneys' fees, arising out of or related to: (i) any misrepresentation or omission of material fact by Subscriber to EADTrust, irrespective of whether such misrepresentation or omission was intentional, (ii) Subscriber's violation of the Subscriber Agreement, (iii) any compromise or unauthorized use of an EADTrust certificate or corresponding Private Key, or (iv) Subscriber's misuse of an EADTrust certificate. If applicable law prohibits Subscriber from providing indemnification for another party's negligence or acts, such restriction, or any other restriction required by law for this indemnification provision to be enforceable, shall be deemed to be part of this indemnification provision.

9.9.2 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify EADTrust and its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by EADTrust or its affiliates and used by the Relying Party, this CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 Term and termination

9.10.1 Term

This CPS and any amendments to this CPS are effective when published to the EADTrust online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CPS and any amendments remain in effect until replaced with a newer version.

9.10.3 Effect of termination and survival

EADTrust will communicate the conditions and effect of this CPS's termination via the EADTrust Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the certificate is revoked or expired, even if this CPS terminates.

9.11 Individual notices and communications with participants

EADTrust accepts notices related to this CPS at the locations specified in Section 1.5.2 of this CPS. EADTrust may allow other forms of notice in its Subscriber Agreements.

9.12 Amendments

9.12.1 Procedure for amendment

This CPS is reviewed at least annually and may be reviewed more frequently. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place that are designed to reasonably ensure that this CPS is not amended and published without the prior authorization of the EADTrust PMA.

9.12.2 Notification mechanism and period

EADTrust posts CPS revisions to its Repository. EADTrust does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice.

9.12.3 Circumstances under which OID must be changed

The EADTrust PMA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute resolution provisions

Any claim, suit or proceeding arising out of this CPS or any EADTrust product or service must be brought in a Spanish court located in Madrid. EADTrust may seek injunctive or other relief in any Spanish court of competent jurisdiction for any actual or alleged infringement of its, its affiliates, or any third party's intellectual property or other proprietary rights.

9.14 Governing law

The activity of EADTrust is governed by Spanish Law and by the Courts of Madrid, unless the user is a consumer, which will result in the application of consumer protection regulations.

9.15 Compliance with applicable law

This CPS is subject to all applicable laws and regulations, including Spanish restrictions on the export of software and cryptography products, and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

EADTrust requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

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

9.16.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force Majeure

EADTrust is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond EADTrust's reasonable control. The operation of the Internet is beyond EADTrust's reasonable control.

9.17 Other provisions

No stipulation.