TSA DISCLOSURE STATEMENT FOR THE ELECTRONIC TIME-STAMPING SERVICE

ancert
Agencia Notarial de Certificación

Document Control

Title:	TSA Disclosure Statement for the Electronic Time-Stamping Service
Document Type:	Choose an item.
name:	TSADS_ENG.docx
Version:	1.0
Status:	Draft
Confidentiality:	Public
Date:	01/10/2020
Author:	Security Office

Review, Approval		
Reviewed by:	Information Security Officer	Date: 02/04/2014
Approved by:	Security Comitee	Date: 02/04/2014

History of changes			
Version	**Date**	**Description of the action**	**Pages**
1.0	04/02/2014	Creation of the document.	

Index

1. Introduction 4

2. Disclosure Text applicable to the Time-Stamping Service 4

2.1. Entire Agreement 4

2.2. TSA contact information 4

2.2.1 Responsible organization 4

2.2.2 Contact details of the organization 4

2.3. Electronic time-stamp types and usage 4

2.3.1 User community and applicability 4

2.3.2 Content of time-stamps 5

2.3.3 Time-stamp request 5

2.3.4 Verification of time-stamps 5

2.4. Reliance limits 5

2.5. Obligations of the subscribers 6

2.6. TSU public key certificate status checking obligations of relying parties 6

2.7. Limited warranty and disclaimer/limitation of liability 6

2.8. Applicable agreements and practice statement 6

2.9. Privacy policy 6

2.10. Refund Policy 7

2.11. Applicable law, complaints, and dispute resolution 7

2.12. TSA and repository licenses, trust marks, and audit 7

1. Introduction

This document contains the essential information to be disclosed in relation to the Time-Stamping service of the Notarial Certification Agency SL Unipersonal (ANCERT).

This document follows the structure defined in Annex B of the ETSI EN 319 421-1 standard.

2. Disclosure Text applicable to the Time-Stamping Service

2.1. Entire Agreement

This document provides high-level statements regarding ANCERT's Qualified Electronic Time-Stamping Service.

This document does not replace or supersede any other policy of ANCERT available at https://www.ancert.com/cps .

2.2. TSA contact information

2.2.1 Responsible organization

Agencia Notarial de Certificación, SL Unipersonal

Paseo General Martínez Campos, number 46.- 6º, Elcano Building

28010 Madrid (Spain)

NIF B-83395988

2.2.2 Contact details of the organization

Any contact with ANCERT, regarding this document can be carried out by the following means:

- Via e-mail to the email address ancert@ancert.com.
- By phone at 902 348 347.

2.3. Electronic time-stamp types and usage

ANCERT's Time-Stamping policy is identified with OID 1.3.6.1.4.1.18920.200.2.1.

The time-stamps issued under this policy are declared as qualified according to Regulation EU 910/2014 and are in accordance with the ETSI EN 1319 411-1 standard.

2.3.1 User community and applicability

ANCERT acts as a TSA for the General Council of Spanish Notaries, Notarial Colleges and Spanish Notaries in the exercise of their public function activity.

Other users must previously contract the service with ANCERT in order to access the Time-Stamping service.

2.3.2 Content of time-stamps

The time-stamps issued by the TSA are in accordance with the profile defined in section 5.2 of the ETSI EN 319 422 standard.

The hash algorithm for time-stamps is SHA-256.

The signing algorithm is *timestampsha256WithRSAEncryption*.

Time-stamps include an extension of type *qcStatements* with the declaration *esi4-qtstStatement-1* according to section 9.1 of ETSI EN 319 422 to indicate that the time-stamp is qualified.

Time-stamps include TSU's electronic certificate (public signing key). The certificate of the TSU is issued by the Certification Authority "ANCERT Certificados Notariales de Sistemas V2" in accordance with the corresponding Certification Practice Statement. TSU's certificate has a validity period of 6 years and an RSA key of length 3072 bits. The use of the TSU key is limited to 5 years.

2.3.3 Time-stamp request

Clients must request time-stamps according to the structure defined in RFC 3161.

The sending protocol for time-stamp requests will be HTTP or HTTPS, according to section 3.4 of RFC 3161.

The cryptographic summary algorithms accepted by ANCERT's TSA are: SHA-256, SHA-512 and SHA-1.

2.3.4 Verification of time-stamps

Certificate revocation status can be checked by OCSP query at the URL:

http://ocsp.ac.ancert.com/ocsp.xuda

Alternatively, it can be also checked by downloading and consulting the CRL of the Certification Authority "ANCERT Certificados Notariales de Sistemas V2" at the URL:

http://www.ancert.com/crl/ANCERTNOT_V2.crl.

URLs to access the OCSP and CRL can be found in the TSU's certificate extensions.

2.4. Reliance limits

ANCERT obtains the time of its systems from a connection to the Royal Navy Observatory (ROA) following the NTP protocol through the Internet.

The accuracy of ANCERT´s time source is 1 second from UTC.

ANCERT maintains records of all TSA operations for 15 years from the issuance of each time-stamp.

2.5. Obligations of the subscribers

The subscriber of the Time-Stamping service must:

- Respect the provisions of the contractual documents signed with ANCERT.
- Comply with ANCERT's Time-Stamping policy.
- Use the service according to the specifications of ETSI EN 319 422.
- Verify the electronic signature of the time-stamp and verify that the certificate associated with the private key with which the TSA signs the stamp has not been revoked, with any of the methods detailed in the section 2.3.4.
- Verify that the cryptographic summary and the policy identifier contained in the time-stamp correspond to those requested.
- Store and keep time-stamps issued by the TSA in case they might be needed in the future.

2.6. TSU public key certificate status checking obligations of relying parties

When a time-stamp is received, the third party must verify the electronic signature of the time-stamp and verify (with any of the methods detailed in section 2.3.4) that the certificate associated with the private key with which the TSA signs the time-stamp, was not revoked at the time of generation of the time-stamp.

2.7. Limited warranty and disclaimer/limitation of liability

ANCERT guarantees, under its sole responsibility, the compliance with all the requirements defined in the Time-Stamping policy.

ANCERT limits its responsibility to the issuance of time-stamps under the conditions of the policy, and in no case will it accept any responsibility for the use of such time-stamps.

ANCERT will not be liable in cases of fortuitous event or force majeure unless there had been serious fault of the entity.

2.8. Applicable agreements and practice statement

The agreements applicable to the qualified electronic Time-Stamping service are the following:

- Certification services contract, which regulates the relationship between ANCERT and the subscriber entity of the qualified electronic time-stamps.
- ANCERT's Time-Stamping Service Practice Statement (DPTSA).
- The General Certification Policy (PG) and ANCERT's Certification Practice Statement (DPC).

The PG, DPC, DPTSA and all the other complementary documentation are accessible at https://www.ancert.com/cps where they are regularly updated.

2.9. Privacy policy

See section 11.4 of the CPS of Notarial Certificates, available at https://www.ancert.com/cps .

2.10. Refund Policy

ANCERT will not refund the cost of the Time-Stamping service in any case.

2.11. Applicable law, complaints, and dispute resolution

Agreements with ANCERT will be under current Spanish law on trust services, as well as under civil and commercial legislation, where applicable.

The competent jurisdiction is defined in Law 1/2000, of January 7, on Civil Procedure.

In case of discrepancy between the parties, the parties will try previous friendly resolution. To this end, the parties must send a communication to ANCERT by any traceable means, to the contact address indicated in point 2.2.2 of this document.

2.12. TSA and repository licenses, trust marks, and audit

ANCERT's TSA services comply with the requirements of Regulation (EU) 910/2014.

ANCERT and its Time-Stamping service are classified in the Spanish list of trusted providers (TSL).

In accordance with the provisions of Regulation EU 910/2014, ANCERT conducts annual audits of its trust services with an accredited entity as CAB (Conformity Assessment Body) and renews the CAR (Conformity Assessment Report) of these services on a biennial basis.