

Qualified and Not Qualified Time Stamp Authority CP_CPS

Document code: ICERT-INDI-TSA_ENG

Version: 2.8

Date: 13/05/2022

CONTENTS

1	INTRODUCTION	7
1.1	Overview	7
1.2	Document name and ID.....	7
1.3	Participants and responsibilities.....	8
1.3.1	Time Stamping Authority	8
1.3.2	Applicant	9
1.3.3	User	9
1.3.4	Authority	9
1.4	Time stamping service usage	9
1.4.1	Permitted uses	9
1.4.2	Prohibited uses.....	9
1.5	Management of Certificate Practice Statement	9
1.5.1	Contacts	9
1.5.2	Parties responsible for approving the CPS.....	10
1.5.3	Approval procedures	10
1.6	Definitions and acronyms.....	10
1.6.1	Definitions.....	10
1.6.2	Acronyms and abbreviations.....	12
2	PUBLICATION AND PRESERVATION.....	14
2.1	Time stamp preservation.....	14
2.2	Publication of certificate information	14
2.2.1	Publication of the CPS.....	14
2.2.2	Publication of the public key for time stamp verification	14
2.2.3	Publication of revocation and suspension lists.....	14
2.3	Publication period or frequency	14
2.3.1	Publication frequency of the CPS.....	14
2.4	Controlling access to public archives.....	15
3	IDENTIFICATION AND AUTHENTICATION	16
3.1	Name.....	16
3.1.1	Type of names	16
3.1.2	Need for names to be meaningful	16
3.1.3	Applicants' anonymity and pseudonym	16
3.1.4	Interpretation rules of the types of names	16
3.1.5	Unequivocalness of the names	16
3.2	Initial identity validation	16
3.3	Identification and authentication for the renewal of the keys and certificates.....	16
3.4	Identification and authentication for revocation or suspension requests	16
4	OPERATIONAL REQUIREMENTS	17
4.1	Request for time stamp emission or verification.....	17
4.1.1	Who can apply for time stamp emission or verification.....	17
4.1.2	Registration process and responsibility	17
4.2	Processing the request	17
4.3	Time stamp issue	18
4.4	Acceptance of the certificate	18
4.5	Key pair and certificate usage	18

- 4.6 Certificate renewal 18
- 4.7 Re-issuing the certificate..... 18
- 4.8 Certificate modification 18
- 4.9 Certificate revocation and suspension 18
 - 4.9.1 Circumstances for revocation 19
 - 4.9.2 Who can request revocation 19
 - 4.9.3 Procedures for revocation request..... 19
 - 4.9.4 Revocation request grace period 19
 - 4.9.5 Time within which CA must process the revocation request..... 19
 - 4.9.6 Requirements for revocation verification..... 19
 - 4.9.7 CRL issuance frequency..... 20
 - 4.9.8 Maximum latency period of the CRL..... 20
 - 4.9.9 On-line revocation/status checking availability..... 20
- 4.10 Services regarding certificate status 20
 - 4.10.1 Operational specifications 20
 - 4.10.2 Service availability 20
- 4.11 Cancelling TS services 20
- 4.12 Third party safekeeping and key recovery 20
- 5 SECURITY AND CONTROL MEASURES 21**
 - 5.1 Physical security 21
 - 5.1.1 Position and construction of the structure 21
 - 5.1.2 Physical access 22
 - 5.1.3 Electric plant and air conditioning 22
 - 5.1.4 Flood prevention and protection 23
 - 5.1.5 Fire prevention and protection 23
 - 5.1.6 Storage media 24
 - 5.1.7 Waste disposal..... 24
 - 5.1.8 Off-site back-up 24
 - 5.2 Procedural controls..... 24
 - 5.2.1 Key roles..... 24
 - 5.3 Staff control 24
 - 5.3.1 Required qualifications, experience and authorisations..... 24
 - 5.3.2 Previous experience control procedures 25
 - 5.3.3 Training requirements 25
 - 5.3.4 Training update frequency 25
 - 5.3.5 Work shift rotation frequency 25
 - 5.3.6 Penalties for unauthorised actions..... 26
 - 5.3.7 Controls on non-employed staff 26
 - 5.3.8 Documents that staff must provide 26
 - 5.4 Management of the control journal..... 26
 - 5.4.1 Types of logged events 26
 - 5.4.2 Control journal processing and back-up frequency 26
 - 5.4.3 Control journal preservation period 26
 - 5.4.4 Control journal protection 26
 - 5.4.5 Control journal back-up procedures..... 27
 - 5.4.6 Control journal back-up system 27
 - 5.4.7 Notification in the event of vulnerability identification 27
 - 5.4.8 Vulnerability assessments 27
 - 5.5 Report storage..... 27
 - 5.5.1 Types of stored reports 27
 - 5.5.2 Report protection..... 27

5.5.3	Report back-up procedures.....	27
5.5.4	Report time stamping requirements	27
5.5.5	Archive back-up system	28
5.5.6	Procedures for obtaining and checking the information stored in the archives.....	28
5.6	TSU private key replacement	28
5.7	TSA private key compromise and disaster recovery.....	28
5.7.1	Accident management procedures.....	28
5.7.2	Machine, software or data corruption.....	28
5.7.3	Procedures in the event the TSA private key is compromised	28
5.7.4	Service distribution in the event of disasters.....	29
5.8	Time stamp service termination	29
6	TECHNOLOGICAL SECURITY CONTROLS.....	30
6.1	Generating a pair of TSU time stamp keys	30
6.1.1	Key algorithm and length	30
6.1.2	Public key quality controls and generation	30
6.2	Private key protection and encryption module engineering controls.....	30
6.2.1	Encryption module controls and standards.....	30
6.2.2	TSA private key control by several people.....	30
6.2.3	TSA private key back-up.....	31
6.2.4	Private key back-up on encryption module.....	31
6.2.5	Private key activation method.....	31
6.2.6	TSA private key destruction method.....	31
6.3	Private key activation data.....	31
6.4	IT security checks	31
6.4.1	Specific computer security requirements	31
6.5	Control system operations	32
6.6	Network security controls	32
7	FORMAT.....	33
7.1	TSU certificate format	33
7.1.1	Version number.....	33
7.1.2	Certificate extensions	33
7.1.3	Signature algorithm OID	33
7.1.4	Name forms.....	33
7.1.5	Name restrictions.....	33
7.1.6	Certificate OID	33
7.1.7	Time stamp format and content	33
7.2	Stamp certificate CRL format	34
7.2.1	Version number.....	34
7.3	OCSP format	34
7.3.1	Version number.....	34
8	COMPLIANCE AUDITS AND ASSESSMENTS.....	35
8.1	Conformity assessment frequency or circumstances	35
8.2	Identity/qualifications of assessor	35
8.3	Relations between InfoCert and CAB.....	35
8.4	Topics covered by assessment.....	36
8.5	Actions taken in case of non conformity	36
9	OTHER BUSINESS AND LEGAL MATTERS.....	37
9.1	Fees.....	37
9.1.1	Time stamp issue fees	37
9.1.2	Time stamp verification fees	37

9.1.3	Fees for other services.....	37
9.1.4	Refund policies.....	37
9.2	Financial responsibilities.....	37
9.2.1	Insurance cover.....	37
9.2.2	Warranty and insurance cover for end subjects.....	37
9.3	Business information confidentiality.....	38
9.3.1	Area of application of confidential information.....	38
9.4	Privacy.....	38
9.4.1	Privacy plan.....	38
9.4.2	Information treated as private.....	38
9.4.3	Processing of personal data.....	38
9.4.4	Privacy information and personal data processing consent.....	38
9.4.5	Data disclosure following requests from the authorities.....	39
9.4.6	Other disclosure reasons.....	39
9.5	Intellectual property rights.....	39
9.6	Representation and warranty.....	39
9.7	Warranty limitation.....	39
9.8	Liability limitation.....	39
9.9	Indemnity.....	40
9.10	Term and termination.....	40
9.10.1	Term.....	40
9.10.2	Termination.....	41
9.10.3	Termination effects.....	41
9.11	Official communication channels.....	42
9.12	Amendments.....	42
9.12.1	Revision history.....	42
9.12.2	Revision procedures.....	45
9.12.3	Notification period and mechanism.....	45
9.13	Disputes.....	46
9.14	Jurisdiction.....	46
9.15	Applicable law.....	46
9.16	Reference standards.....	47
9.17	Various regulations.....	47
9.18	Other provisions.....	47
Annex A	48
	Time stamp root "InfoCert Time Stamping Authority 2".....	48
	Qualified time stamp root "Qualified InfoCert Time Stamping Authority 2".....	51
	Time stamp root "InfoCert Time Stamping Authority 3".....	55
Caution	59

ILLUSTRATIONS INDEX

Figura 1 – Infocert Datacenter and Disaster Recovery site location	22
---	-----------

1 INTRODUCTION

1.1 Overview

This manual is intended to describe the rules and operational procedures adopted by InfoCert's digital certification structure for the provision of a qualified and not qualified times stamping trust service according to eIDAS Regulation.

InfoCert provides digital time stamping service for both digitally signed and unsigned documents.

Generally, the time stamping service allows you to establish the existence of a computer document before a certain time, associating a date and time from a certified time source with the digital evidence obtained from the document. Digital evidence is subject to time stamping when its associated timestamp is generated: the timestamp is a digitally signed data record that securely and verifiably links any digital document to a time reference (date and time).

The timestamp is signed and issued by a trust service provider that provides time stamping systems (Time Stamping Authority (TSA)) that certifies the trust system keys (Time Stamp Unit (TSU)) to which users direct their requests according to need; anyone who has requested and stored a time stamp for a particular document will subsequently be able to prove that this document actually existed at the date/time reported in the stamp signed by that TSU/TSA certification chain.

In particular, the digitally signed document time stamp allows for the verification and validation of the digital signature, even if the author's certificate is expired or revoked, provided that the time stamp was assigned to the document when the certificate was valid.

The service provided by InfoCert meets BTSP policy as defined in ETSI319421 [2] identified by the OID.

DESCRIPTION	OID
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy(1)	0.4.0.2023.1.1

1.2 Document name and ID

This document is called "Qualified and not qualified Time Stamping Service – Certificate Practice Statement" and is characterised by the document code: **ICERT-INDI-TSA-ENG**. The version and issuing level can be found at the bottom of each page.

The document is associated with the *Object identifier* (OID) **1.3.76.36.1.1.40**. This OID identifies:

DESCRIPTION	OID
InfoCert	1.3.76.36
Certification-service-provider	1.3.76.36.1
Certificate-policy	1.3.76.36.1.1
Qualified time stamping service - certificate policy	1.3.76.36.1.1.40
Not qualified time stamping service - certificate policy (certificates for non-InfoCert TSUs)	1.3.76.36.1.1.41
Not qualified time stamping service - certificate policy	1.3.76.36.1.1.42

In addition, all the certificates comply with the instruction of AgID Resolution n. 121/2019, effective since July 5, 2019 and contain an additional PolicyIdentifier element, with value AgIDcert (OID 1.3.76.16.6) in the CertificatePolicies field (OID 2.5.29.32).

1.3 Participants and responsibilities

1.3.1 Time Stamping Authority

The **Time Stamping Authority** is the trusted third party that provides the time stamping service.

InfoCert is the trust service provider (**TSA**) that provides the qualified and not qualified time stamping service (TSU) by operating in accordance with the eIDAS Regulation i and the European Telecommunications Standards Institute standards (ETSI).

Complete data of the organisation that acts as CA are as follows:

Company name	InfoCert – Joint-stock company Company under the management and coordination of Tinexta S.p.A.
Registered office	Piazza Sallustio no.9, 00187, Rome (ROME)
Headquarters	Via Marco e Marcelliano no.45, 00147, Rome (ROME)
Legal representative	Danilo Cattaneo In his capacity as Managing Director
Telephone no.	+39 06 836691
Registered with the Register of Companies under no.	Tax Code 07945211006
VAT number	07945211006
Website	https://www.infocert.it

1.3.2 Applicant

The **Applicant** is the natural or legal person to whom the time stamp is provided and who enters into the contract with InfoCert.

1.3.3 User

The individual who receives a digital document that is time stamped and relies on the validity of the stamp must evaluate the correctness and validity of the document itself, in the contexts where it is used.

1.3.4 Authority

1.3.4.1 Agenzia per l'Italia Digitale - AgID

The Agenzia per l'Italia Digitale (**AgID**), is the trust service provider authority in compliance with article 17 of the eIDAS Regulation . In this role, AgID monitors qualified trust service providers established in Italy to ensure they comply with the requirements set out in the Regulation.

1.3.4.2 Conformity Assessment Body

The conformity assessment body (**CAB**), is an accredited body as provided for under the eIDAS Regulation in charge of assessing the conformity of qualified trust service providers and their qualified trust services in line with the applicable regulations and standards.

1.4 Time stamping service usage

1.4.1 Permitted uses

Time stamps issued by InfoCert, as specified in this CPS, are qualified under the eIDAS Regulation.

The certificate issued by the TSA will be used to verify the stamp.

InfoCert provides the GoSign product, downloadable from the InfoCert site, to check stamps. Additional verification products may be available on the market with features and limitations specified by the manufacturer.

1.4.2 Prohibited uses

Use outside of the limits and contexts specified in the CPS and contracts is prohibited.

1.5 Management of Certificate Practice Statement

1.5.1 Contacts

InfoCert is responsible for definition, publication and update of this document. Questions, claims, observations and requests for clarification regarding this CPS must be sent to the address and person indicated below:

InfoCert S.p.A.**Digital Certification Service Manager**

Piazza Luigi da Porto no.3

35131 Padova

Telephone: +39 06 836691

Fax: +39 06 23328861

Digital Signature Call Centre: see the link <https://help.infocert.it/contatti/>Web: <https://www.firma.infocert.it>e-mail: firma.digitale@legalmail.it**1.5.2 Parties responsible for approving the CPS**

This Certificate Practice Statement has been approved by the Company's management following a review by the Head of Security and Policies, the Privacy Manager, the Head of Certification Services, the Legal Office and the Consultancy department.

1.5.3 Approval procedures

Drafting and approval of this Certificate Practice Statement are carried out in accordance with the procedures described in the Company's Quality Management System ISO 9001:2015.

At least once a year, the Trust Service Provider checks the compliance of this Certificate Practice Statement with its certification service process.

1.6 Definitions and acronyms**1.6.1 Definitions**

The definitions used when drawing up this document are listed below. For the terms defined by the eIDAS Regulation [1] and CAD [2] please refer to the definitions established therein. Where appropriate, the corresponding English term generally used in journalism, in standards and technical documents, is given in square brackets.

Expiry	Definition
CAB – Conformity Assessment Body	Accredited body as foreseen under the eIDAS Regulation capable of carrying out the conformity assessment of the qualified trust service provider and of their qualified trust services. It issues the CAR.
Electronic signature certificate	An electronic certificate that links the validation data of an electronic signature to a TSU.
Private key	The element of the pair of asymmetrical keys, used by the TSU to sign a time stamp (see CAD ii).
Public Key	The element of the pair of asymmetrical keys intended to be made public, with which the time stamp is verified.

Validation	The process of verifying and confirming the validity of a time stamp.
Validation data	Data used to validate a time stamp.
Digest (imprint)	Message imprint after applying a hash algorithm.
Electronic Document	Any content stored in electronic format, especially text or sound, visual or audio-visual recordings (see eIDAS [1]).
Electronic signature	Data in electronic form, enclosed or connected by logical association with other electronic data and used by the TSU to issue a time stamp.
Certificate Revocation List - CRL	This is a list of certificates that have been rendered "invalid" before their natural deadline. The operation is called revocation if permanent, suspension, if temporary. When a certificate is revoked or suspended, its series number is added to the CRL, which is then published in the public register.
Operating manual [certificate practice statement]	The Operating Manual defines the procedures that the TSP applies when carrying out the service. When the Manual was being drawn up, the indications expressed by the Supervisory Authorities and those found in international literature were followed.
Time stamp	Electronic data that connects other electronic data with time evidence demonstrating that this data existed at that time.
On-line Certificate Status Protocol (OCSP)	Protocol defined by the IETF in the RFC 6960; it allows the applications to check the certificate's validity more rapidly and punctually compared to the CRL, of which it shares the data.
PKCS#10	Acronym for Public Key Cryptography Standards, it is a set of standards for public key cryptography developed by RSA Labs: they define the syntax of digital certificate and encrypted messages, in particular PKCS#10 defines the structure of the public key certificate request for a pair of asymmetric keys.
Trust service provider	A natural or legal person who provides one or more trust services, either as a qualified or unqualified trust service provider (see eIDAS i)
Qualified trust service provider	A trust service provider who provides one or more qualified trust services and to whom the supervisory body grants the title of qualified trust service provider (see eIDAS i).
Certificate revocation or suspension	This is the operation with which the CA cancels the validity of the certificate before its natural deadline.
Trust service	An electronic service normally provided at a fee and consisting in the following elements: <ul style="list-style-type: none"> a) creation, verification and validation of electronic signatures, electronic seals or temporary electronic validations, electronic services of certificate forwarding and certificates relating to these services; or b) creation, verification and validation of website authentication certificates; or c) storage of signatures, seals or electronic certificates relating to these services (see eIDAS i)
Qualified trust service	A trust service that meets the relevant requirements established in the Regulation (see eIDAS i).

SHA-256	The SHA acronym stands for Secure Hash Algorithm and is a cryptographic function used to calculate the hash or digest or imprint. 256 is the number of bits in the resulting message.
Coordinated Universal Time	Time-scales with precision to the second as defined in ITU-R Recommendation TF.460-5.
Temporary electronic validation	Data in electronic format that connects other data in electronic format to a particular time and date, in order to prove that the latter existed at that moment in time (see eIDAS i).
Qualified temporary electronic validation	A temporary electronic validation that meets the requirements found in article 42 of the eIDAS Regulation (see eIDAS i).
X.509	Standard for defining the format of the digital public key certificate format. It also defines the characteristics of a Public Key Infrastructure (PKI).

1.6.2 Acronyms and abbreviations

Acronym	Description
AgID	Agenzia per l'Italia Digitale: (Agency for Digital Italy) Trust Service Providers Supervisory Board
BTSP	Best Practices Time-Stamp Policy - see ETSI319421
CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Digital Administration Code
CAR	Conformity Assessment Report
CC	Common Criteria
CRL	Certificate Revocation List
DMZ	Demilitarised Zone
eIDAS	Electronic Identification and Signature Regulation
ETSI	European Telecommunications Standards Institute
HSM	Hardware Secure Module: it is a security device for the creation of the signature, with functions that are similar to smart cards, but with a larger memory and superior performance
ISO	International Organisation for Standardisation: founded in 1946, ISO is an international organisation made up of national bodies for standardisation
LDAP	Lightweight Directory Access Protocol: protocol used to access the certificates register;
OID	Object Identifier: consists of a sequence of numbers, registered according to the procedure indicated in the ISO/IEC 6523 standard which identifies a certain object within a hierarchy
PEC	Certified E-mail

PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure: group of resources, processes and technological means that allow trusted third parties to check and/or guarantee the identity of a subject, as well as associate a public key to a subject
RFC	Request for Comment: document that holds information or specifications regarding new research, innovations and methods in the IT world, requested to be assessed by the community by the writers
SGSI	Information Security Management System
SSCD - QSSCD	Secure Signature Creation Device: device for the creation of an electronic signature. Qualified Secure Signature Creation Device: qualified device for the creation of an electronic signature.
TSA	Time-Stamping Authority: Trust service provider using one or more time stamp emission systems - see ETSI319421
TST	Time-Stamp Token: term used in international advertising for the time stamp
TSU	Time-Stamping Unit: a set of hardware and software managed as a single time stamping system consisting of only one active key - see ETSI319421
TSP	Trust Service Provider see Trust service provider
UTC	Coordinated Universal Time as defined in ITU-R TF.460-6 (2000) - see ETSI319421
X509	ITU-T Standard for the PKIs

2 PUBLICATION AND PRESERVATION

2.1 Time stamp preservation

All time stamps emitted by a validation system are stored in a non-editable digital archive for twenty years.

2.2 Publication of certificate information

2.2.1 Publication of the CPS

This document, the list of certification key certificates and other information relating to the TSA provided for by law are published in a list of certifiers (at link <https://eidas.agid.gov.it/TL/TSL-IT.xml>) and on the Certification Authority's website (see § 1.5.1).

2.2.2 Publication of the public key for time stamp verification

The integrity and authenticity of the TSU server public key is guaranteed as it is distributed by issuing a public key certificate:

- The certification request is issued by authorised personnel and forwarded to CA InfoCert dedicated to the certification of time stamp keys.
- The CA generates the certificate.

The time stamp certificate format, containing the TSU public key, meets that specified in ETSI319422 [3]; in this way it, full readability and verifiability is guaranteed in the context of eIDAS and Italian legislation.

The public key used by TSU is distributed through the certificate.

2.2.3 Publication of revocation and suspension lists

The revocation and suspension lists are published in the public register of certificates accessible with LDAP protocol at: <ldap://ldap.infocert.it> or with http protocol at: <http://crl.infocert.it>. This access can be made via the software made available by InfoCert and/or the functions found in the products on the market which interpret the LDAP and/or HTTP protocol.

2.3 Publication period or frequency

2.3.1 Publication frequency of the CPS

Frequency of publication of the Certificate Practice Statement varies to reflect any changes that have occurred. For major changes, the CA must undergo an audit by an accredited CAB, submit the certification report (CAR—Conformity Assessment Report)

and the Certificate Practice Statement to the Supervisory Authority (AgID) and wait for a publication permission to be granted.

2.4 Controlling access to public archives

The information regarding the published certificates and certificate practice statement are public, the CA did not place any restrictions on access to their reading and implemented all counter-measures to prevent unauthorised changes/deletion.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Name

3.1.1 Type of names

The key used by the TSU in the certificate is identified with the assigned Distinguished Name (DN), which should therefore be valued and compliant with the X500 standard. Certificates are issued according to ETSI standards for issuing qualified certificates for time stamping.

3.1.2 Need for names to be meaningful

The Distinguished Name (DN) certificate contains a name that identifies the TSU used, the month and year of issue.

3.1.3 Applicants' anonymity and pseudonym

n/a

3.1.4 Interpretation rules of the types of names

InfoCert complies with the X500 standard

3.1.5 Unequivocalness of the names

The Distinguished Name (DN) certificate contains a name that identifies the TSU used, the month and year of issue: each TSU uses a unique certificate.

3.2 Initial identity validation

n/a

3.3 Identification and authentication for the renewal of the keys and certificates

n/a

3.4 Identification and authentication for revocation or suspension requests

n/a

4 OPERATIONAL REQUIREMENTS

4.1 Request for time stamp emission or verification

4.1.1 Who can apply for time stamp emission or verification

The time stamping service is intended to address time stamp emission or verification request for electronic documents from the TSU server by means of properly configured software modules.

The request for time stamp emission or verification may be made by the **Applicant/User** using the signature/verification software provided by InfoCert, which allows you to affix the timestamp to digitally signed and non-signed documents, and allows immediate verification.

The Applicant may use its own software through a protocol defined in RFC 3161, RFC 5816 and profiled by the ETSI 319 422 standard using URLs and credentials agreed with InfoCert.

Once the request has been accepted and registered and proper checks are carried out, the TSU server processes it, generates the time stamp and sends it back to the Applicant/User.

Note: the InfoCert certifier site has stamp affixing and verification software, for both a signed document or an unsigned document.

4.1.2 Registration process and responsibility

In the process, the different figures involved have different roles and run parallel with the successful outcome of the issuance:

- The Applicant/User is responsible for submitting the request for time stamp issuance or verification through the software modules for this purpose provided by the InfoCert trust service provider.
- InfoCert is ultimately responsible for the success of the time stamp generation process.

4.2 Processing the request

The request is processed as follows:

- The Applicant submits, through TSA's procedures, a time stamp request for the electronic document to the TSU server, eventually viewing it;
- the request contains the imprint of the electronic document to be stamped using the SHA-256 imprint algorithm (secure hash algorithm 256-bit).

4.3 Time stamp issue

The time stamp is automatically issued by a secure electronic system (TSU server), managed by TSA, able to:

- accurately calculate the date and time of time stamp generation with reference to Coordinated Universal Time (UTC);
- generate the data record containing the specified information [iii];
- digitally sign (in the technical meaning of the term) the data record.

Upon receipt of the request, the time stamp is issued as follows:

- The TSU, upon receipt of the time stamp request, generates the data record as defined in [iii]: this record contains, amongst the various information, the same imprint and the current date/time;
- The TSU server signs the generated data record, obtaining the time stamp;
- When the time stamp generation procedure has successfully completed, the latter is sent to the Subject.

4.4 Acceptance of the certificate

n/a

4.5 Key pair and certificate usage

n/a The pair of keys and stamp certificate are solely used to sign the association between the date-time and the imprint of the document.

4.6 Certificate renewal

n/a The certificate does not provide for renewal.

4.7 Re-issuing the certificate

A new certificate is issued for each TSU every three months.

4.8 Certificate modification

n/a

4.9 Certificate revocation and suspension

The revocation or suspension of a certificate removes its validity prior to the established

expiry date and means the stamps placed after the revocation has been published, are no longer valid. Revoked or suspended certificates are added to the revocation and suspension list (CRL) signed by the TSA who issued them, published in the register of certificates on an established periodic basis. The TSA can impose an unscheduled issuing of the CRL under particular circumstances. The revocation and suspension is effective as of the list publication date, proven by the event registration date in the TSA Audit Journal.

The information on the revocation status remains available at the Certification Authority for 20 years after the expiration of the TSA root certificate through the issuance and the preservation of the latest CRL.

4.9.1 Circumstances for revocation

The conditions under which the time stamp certificate may be revoked are:

1. the private key has been compromised, that is, one of the following cases has arisen:
 - the secure signature device that contains the key has been violated;
 - key or its activation code (PIN) secrecy has been breached;
 - some kind of event has occurred that has compromised the level of the key's reliability.
2. significant failure to comply with this document is verified.

4.9.2 Who can request revocation

The certificate may be revoked or suspended by TSA for reasons stated in § 4.9.1.

4.9.3 Procedures for revocation request

n/a

4.9.4 Revocation request grace period

The grace period of the CRL is the period of time between the time of publication by the TSA of the next CRL and the time when the current CRL expires. In order not to cause disruption to any involved party, this period is longer than the time period TSA needs to generate and publish a new CRL. This way, the current CRL remains valid at least until it is replaced by the new CRL.

4.9.5 Time within which CA must process the revocation request

The request is processed immediately as soon as the TSA has verified the reason for revocation.

4.9.6 Requirements for revocation verification

n/a

4.9.7 CRL issuance frequency

The revoked or suspended certificates are added to a revocation and suspension list (CRL) signed by TSA and published in the Public Register. The CRL publication is scheduled every hour (ordinary issuing). Under particular circumstances, the TSA may impose an unscheduled issuance of the CRL (immediate extraordinary issue), for example in the case where the revocation or suspension of a certificate occurs if there is a suspicion that the private key's secrecy has been compromised (immediate revocation or suspension). The CRL is always issued in its entirety. When the CRL is published, it is certified by using the date provided by the Time Stamping Authority InfoCert system as temporal reference and this recording is made in the control journal. Each element in the CRL list contains the date and time of revocation or suspension in the specific extension. The CRL to be consulted for the specific certificate is indicated in the certificate itself in compliance with current standards.

4.9.8 Maximum latency period of the CRL

The time that elapses between the revocation or suspension request and its completion with publication of the CRL is no more than one hour.

4.9.9 On-line revocation/status checking availability

As well as the publication of the CRL in the LDAP registers and http, InfoCert also makes an OCSP service available to verify certificate status. The service's URL is shown on the certificate. The service is available 24/7.

4.10 Services regarding certificate status

4.10.1 Operational specifications

Information on the status of the certificates is available via CRL and the OCSP service. The serial number on the revoked certificate remains in CRL even after the certificate's validity has expired and at least until the TSA certificate expires.

The information provided by the OCSP service for the certificates is updated with the most recent CRL published.

4.10.2 Service availability

The OCSP service and CRLs are available 24/7.

4.11 Cancelling TS services

n/a

4.12 Third party safekeeping and key recovery

n/a

5 SECURITY AND CONTROL MEASURES

TSP InfoCert has developed an information security system for the digital certification service. The implemented security system is divided into three levels:

- a physical level that aims to guarantee the security of the environments in which the TSP manages the service,
- a procedural level, with strictly organisational aspects,
- a logical level, via the arrangement of technological hardware and software measures that deal with the problems and risks relating to the kind of service and infrastructure used.

This security system was created to prevent risks deriving from system, network and application malfunctions, as well as the unauthorised interception or change of data.

A copy of the InfoCert security policy can be requested from the certified e-mail address infocert@legalmail.it.

InfoCert Security policies are reviewed no less than yearly; they are also updated against any significant changes. Each revision is tracked in the document even when no changes had to be made.

5.1 Physical security

The measures adopted provide adequate security guarantees regarding:

- Characteristics of the building and construction;
- Active and passive theft prevention systems;
- Physical access control;
- Electrical power supply and air conditioning;
- Protection against fires;
- Protection against flooding;
- Magnetic support storage methods;
- Magnetic support storage sites.

5.1.1 Position and construction of the structure

The InfoCert Data Centre is located in Padua. The Disaster Recovery site is located in Modena and is connected to the Data Centre mentioned above via a specific and redundant connection on two different 40 Gbit/s MPLS circuits that can be upgraded to 100 Gbit/s.

Protected areas with the highest levels of security, both physical and logical, within

which there is certified IT equipment that makes up the heart of the digital certification services, timestamp and remote and automatic signature are located within both.

For services that need business continuity with RTO/RPO values close to zero, some components of the time stamping services relating to publication of the CRLs, the OCSP and some Front-End services are hosted on AWS cloud, respectively, in Frankfurt Europe, Ireland Europe and Milan Europe Region.

AWS has certifications of conformity in accordance with the ISO/IEC 27001: 2013, 27017: 2015, 27018: 2019 and ISO/IEC 9001: 2015 standards.



Figure 1 - InfoCert Data Centre and Disaster Recovery site location

5.1.2 Physical access

Access to the Data Centre is regulated by InfoCert security procedures. There is a bunker area within the Data Centre where the CA systems are located and for which yet another level of security is required.

5.1.3 Electric plant and air conditioning

The site that houses the InfoCert Data Centre in Padua, while not being certified, has the characteristics of a 3 tier Data Centre.

The technical rooms are fitted with an electric power supply system designed to prevent breakdowns and, above all, disservices. The system's power supply includes the most modern technology with a view to increasing reliability and ensuring redundancy in the most essential functions for the services provided.

The power supply infrastructure includes:

- UPSs, fitted with AC accumulators;
- AC voltage available (220-380V AC);
- Redundant power supply cabinets with protected lines and with a size suitable for the agreed absorption;
- Emergency generator service;
- Automatic commutation system and synchronisation between generators, network and batteries (STS).

Each technological cabinet installed at the Data Centre uses two electrical lines that guarantee the HA in the event that one of the two available lines is interrupted.

The technological cabinet is monitored remotely; continuous controls are carried out on the status of the electric lines (on/off) and the electrical power absorbed (each line should not exceed 50% of the load).

The technical area is normally maintained between 20° and 27° with a relative humidity level between 30% and 60%. The plants are fitted with condensation batteries with condensation collection and drainage system and controlled by anti-flooding probes. The entire conditioning system is served by emergency generators in the event of a power cut. Cabinet cooling capacity is guaranteed with a maximum foreseen load of 10kW and a maximum of 15kW on two cabinets side by side.

5.1.4 Flood prevention and protection

The area where the property is located does not present environmental risk from any “dangerous” installations in the vicinity. When the building was being designed, specific measures were taken to insulate the buildings from potential danger, such as those housing the electrical generator and central heating plant.

The area that houses the equipment is on the ground floor in a raised position compared to the road level.

5.1.5 Fire prevention and protection

The Data Centre has a smoke detection system managed by an analogical power station referred to as NOTIFIER, with optical sensors positioned in the room and ceiling and air sample sensors installed underground and in the air ducts.

The automatic fire detection system is connected to automatic NAFS125 and PF23 ecological gas extinguishing plants and, in certain rooms, with sprinkler extinguishing systems.

Should the two detectors trigger in the same area, the extinguishing discharge is applied to the area involved.

Each fire extinguishing compartment has a specific extinguishing plant.

There are also portable extinguishers in compliance with current regulations and laws.

The primary air ducts serving the equipment rooms are fitted, in correspondence with the crossings of fire proof compartments, with fire proof shutters that can be activated by the automatic fire alarm system.

5.1.6 Storage media

As far as the storage platform is concerned, the solution provides the use of Net App (FAS 8060) systems for the NAS part. For the SAN part instead, an infrastructure based on Infinidat technology was implemented that includes n.2 InfiniBox enclosure of generation F4000 and F6000; for the CA, the infrastructure is based on Pure Storage technology.

5.1.7 Waste disposal

InfoCert is ISO 14001 certified for the sustainable environmental management of its production cycle, including recycling and the sustainable disposal of waste. As far as the IT content of electronic waste is concerned, all the media, prior to disposal, is cleaned in compliance with established procedures, that is, using certified sanitation companies.

5.1.8 Off-site back-up

This is done at the Disaster Recovery site, with an EMC Data Domain 4200 device on which the Padua site primary Data Domain replicates the back-up data.

5.2 Procedural controls

5.2.1 Key roles

The key roles are held by individuals with the necessary experience, professionalism and technical and legal skills, that are continually checked on an annual basis.

The list of names and the organisation chart of the individuals in key roles was deposited at the AgID upon first accreditation and is constantly updated to follow the corporate organisation's natural evolution.

5.3 Staff control

5.3.1 Required qualifications, experience and authorisations

Once the yearly Human Resources plan has been drawn up, the Head of the Department/Business unit identifies the specifications and resource skills to be added (*job profile*). Following this, and in conjunction with the selection manager, the recruitment and selection process begins.

5.3.2 Previous experience control procedures

The identified candidates participate in the selection process through an initial cognitive-motivational interview with the head of HR and a second technical interview with the head of the Department/Business unit, aimed at checking the skills stated by the candidate. Further verification tools are exercises and tests.

5.3.3 Training requirements

As a guarantee that no single individual can singularly compromise or alter the global system security or do anything unauthorised, system operating management is assigned to different people, with separate, clearly defined roles. The staff member assigned to the certification service programming and distribution is an InfoCert employee and was selected on the basis of his/her experience in programming, creating and managing IT services as well as of his/her reliability and confidentiality. Training is periodically planned to develop familiarity with the assigned roles. In particular, before starting work, personnel are trained in order to provide every kind of skill (technical, organisational and procedural) required to carry out the tasks assigned.

5.3.4 Training update frequency

Training needs are analysed at the start of each year in order to define the training activities to be provided throughout the year. The analysis is organised as follows:

- Meeting with Management to collect the data relating to the training requirements needed to satisfy company aims;
- Interview with managers to gather data on training requirements specific to their own areas;
- Collected data is returned to Company Management for training plan closure and approval.

Within the month of February, the defined Training Plan is shared and published.

5.3.5 Work shift rotation frequency

The presence on site or in agile work mode (smart working) is distributed over a time slot from 08:00 to 19:00 from Monday to Friday.

The supervision of the production environments during the night and during the holidays is guaranteed through an on-call shifts plan that is drawn up by the business unit manager monthly, at least 10 days in advance. Depending on the need, the interventions can be conducted remotely (tele-intervention) or request access to the premises.

Without prejudice to the possession of the necessary technical and professional requirements, the Company aims to alternate as many workers as possible in the on-call shifts plan, giving priority to employees who request to do so.

5.3.6 Penalties for unauthorised actions

Please refer to the “Metalworkers and private industry plant installation National Collective Bargaining Agreement” for the procedures on imposing penalties.

5.3.7 Controls on non-employed staff

External employee access is managed by specific company policy.

5.3.8 Documents that staff must provide

When hired, the employee must provide a valid copy of an identification document, a valid health card and a passport photo for his/her access badge. S/he will subsequently have to fill out and sign the authorisation to process personal data and the commitment to not disclose confidential news and/or documents. Lastly, s/he must read the InfoCert’s Code of Ethics and Netiquette.

5.4 Management of the control journal

Events related to TSA management, certificate life, and time source events are collected in the control journal as required by the Regulation and Technical Rules.

All events concerning the signature devices customizations are recorded.

All physical accesses to high security zone, in which server is located, are recorded

5.4.1 Types of logged events

Security events are recorded as well as start up and shut down, system crashes and hardware faults, firewall and router activities and attempts to access the PKI systems.

Event related to TSU keys and certificates are recorded.

All events related to the synchronisation and recalibration of TSU clocks with UTC coordinated universal time are recorded.

Each event is saved with system date and time of the event.

5.4.2 Control journal processing and back-up frequency

Data processing and grouping as well as back-up on the compliant InfoCert storage services of electronic documents takes place at least monthly.

5.4.3 Control journal preservation period

The control journal is kept for at least 20 years by the CA.

5.4.4 Control journal protection

Control journal protection is guaranteed by the InfoCert electronic documents Storage System, compliant with electronic documents storage applicable legislation.

5.4.5 Control journal back-up procedures

The InfoCert Storage Services compliant with electronic documents storage applicable legislation, implements a back-up policy and procedure, as set out in the manual for these services.

5.4.6 Control journal back-up system

Event logs are collected via automatic custom procedures; back-up occurs in the manner provided for by the InfoCert Storage Services compliant with electronic documents storage applicable legislation, and described in the security manual for these services.

5.4.7 Notification in the event of vulnerability identification

n/a

5.4.8 Vulnerability assessments

InfoCert periodically carries out vulnerability assessments and penetration tests on the System. Based on the results, it implements all the counter-measures to ensure applications are secure.

5.5 Report storage

5.5.1 Types of stored reports

Reports related to the most important events of a Certification Authority are drafted and stored. Reports are stored at least for 20 years by the Certification Authority in the InfoCert Storage Services compliant with electronic documents storage applicable legislation.

5.5.2 Report protection

Protection is guaranteed by the InfoCert Storage Services compliant with electronic documents storage applicable legislation.

5.5.3 Report back-up procedures

InfoCert Storage Services compliant with electronic documents storage applicable legislation, implements a back-up policy and procedure, as set out in the security manual for the above mentioned services.

5.5.4 Report time stamping requirements

n/a

5.5.5 Archive back-up system

Reports are collected via automatic custom procedures; back-up occurs in the manner provided for by the InfoCert compliant storage service and described in the security manual for the above mentioned services.

5.5.6 Procedures for obtaining and checking the information stored in the archives

The data are all stored in the compliant InfoCert's Electronic Document Retention Services , which provide for timely checks on system status and data integrity. Data storage is performed in accordance with the standard.

5.6 TSU private key replacement

Each pair of keys used for time stamping is uniquely associated with the system providing the service. Time stamp keys (TSU keys) are replaced every six months before the expiration of the certificate without revoking the previous one.

5.7 TSA private key compromise and disaster recovery

5.7.1 Accident management procedures

The TSP has described the accident management procedures under ISO 27000 certified SGSI. Any accident, as soon as it is reported, is subject to strict analysis, identification of corrective counter-measures and reported by the service manager. The report is digitally signed and sent to the the compliant InfoCert's Electronic Document Retention Services ; a copy is also sent to the AgID, together with the declaration of actions to be taken aimed at eliminating the causes that may have given rise to the accident, if under the control of InfoCert, as set forth in article 19 of the Regulation.

5.7.2 Machine, software or data corruption

In the event of HSM signature security device fault containing the certification keys, the spare copy of the certification key is used, suitably stored and kept, and there is no need to revoke the corresponding TSA certificate.

Software and data are subject to regular back-ups as provided by internal procedures.

5.7.3 Procedures in the event the TSA private key is compromised

A compromised certification key is considered a particularly serious event as it would invalidate the issued certificates and the revocation status information signed using that key. Particular focus is, therefore, placed on protecting the certification key and all the system's development and maintenance activities that can have an impact on it.

Despite being a rare event, InfoCert has prepared a detailed procedure to be followed under the ISO 27000 certified SGSI, giving evidence to the CAB.

Once the TSA private key has been compromised, InfoCert will proceed promptly

- to inform AgID, the Italian Supervisory Body, for the removal of the key from the TSL and the CAB,
- to notify customers through direct communication, where possible, and through communication on the InfoCert website,
- to shut down the service with the compromised key and revoke the impacted certificates, possibly to proceed with the issuance and accreditation of a new TSA root and to reliably provide information on the revocation status of the certificates.

InfoCert described the procedure to be followed in the event of compromised key, under the ISO 27000 certified SGSI, also informing the AgID and CAB.

5.7.4 Service distribution in the event of disasters

InfoCert has adopted the necessary procedures to ensure service continuity even in extremely difficult or disastrous situations.

5.8 Time stamp service termination

In the event the time stamp service is terminated, InfoCert will communicate its intention to the Supervisory Body (AgID) and to the Conformity Assessment Body (CAB) at least 6 months in advance, indicating, if necessary, the certificates and relevant documents register holder.

In the event of TSA termination, information on the revocation status will be provided by issuing the latest CRL.

More details can be found in the TSP Termination Plan document of the Digital Certification and Time Validation Services available at InfoCert.

6 TECHNOLOGICAL SECURITY CONTROLS

6.1 Generating a pair of TSU time stamp keys

The time stamp is signed with an asymmetric algorithm from a private key stored on a secure hardware device and the corresponding public key certified by an InfoCert Certification Authority dedicated to this service (TSA).

The pair of asymmetric keys is generated within a hardware encryption device (HSM) compliant with the security requirements provided by ETSI319421 [26].

The TSU asymmetric key pair generation devices can only be activated by authorised operators, working in pairs, who unlock the encryption device by inserting a pair of smart cards accompanied by the PIN.

Private keys are generated and stored in encryption devices so as to prevent them from being exported.

6.1.1 Key algorithm and length

The pair of asymmetrical certification keys is generated inside the hardware encryption device mentioned above. The RSA asymmetrical algorithm with key length no less than 2048 bits is used.

6.1.2 Public key quality controls and generation

The devices used are certified according to high security standards (see § 6.2.1) and ensure that the public key is correct and random. The CA, before issuing the certificate, verifies that the public key has not been used yet.

6.2 Private key protection and encryption module engineering controls

6.2.1 Encryption module controls and standards

The encryption modules used by InfoCert for certification keys (TSAs) are FIPS 140 Level 3 and Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 validated in Europe.

6.2.2 TSA private key control by several people

Access to the devices containing the certification keys only takes place with two people authenticated at the same time.

6.2.3 TSA private key back-up

The back-up of the keys is contained in a safe which can only be accessed by personnel not permitted to access the HSM devices. Any restore, therefore, requires both those staff members who have access to the devices and those who have access to the safe.

6.2.4 Private key back-up on encryption module

The certification key is generated and backed-up in a protected area of the encryption device that inhibits its exportation. Furthermore, the device's operating system, in the event of its protection being forced, blocks the device or makes it illegible.

6.2.5 Private key activation method

The time stamp service can only be activated by authorised operators using a series of passwords and having a number of personal encryption devices.

Once activated, the system does not need additional interactive login procedures except to stop it and reactivate it for maintenance purposes.

6.2.6 TSA private key destruction method

InfoCert personnel assigned to this role deals with the destruction of the private key when the certificate has expired or has been revoked, according to the security procedures provided for by the security policies and device manufacturer's specifications.

6.3 Private key activation data

Please see paragraphs 4.2 .

6.4 IT security checks

6.4.1 Specific computer security requirements

The computer operating system used in certification activities for key generation, certificate generation and certificate register management are secured (hardening), that is, they are configured in order to minimise the impact of any vulnerability by eliminating all the functions that are of no use for the operation and management of the CA.

System administrators, specifically appointed in compliance with current legislation, login via an on-demand root application that only allows root user privileges to be used upon individual authentication. Accesses are tracked, logged and stored for 12 months.

6.5 Control system operations

InfoCert considers secure information processing to be strategically important and recognises the need to constantly develop, maintain, control and improve an Information Security Management System (SGSI) in compliance with ISO/IEC 27001 standard.

InfoCert received ISO/IEC 27001:2005 certification in March 2011 for EA:33-35 activities. In March 2015 it was certified for the new version of the ISO/IEC 27001:2013 standard. Procedures and controls are provided in SGSI for:

- Asset Management;
- Access Control;
- Physical and Environmental Safety;
- Operation Activities Security
- Communications Security;
- System Acquisition, Development and Maintenance;
- Accident Management;
- Operational Continuity.

All the procedures are approved by the relative managers and shared internally in the InfoCert document management system.

6.6 Network security controls

InfoCert created a network security infrastructure for the certification service, based on the use of firewall mechanisms and SSL protocol in order to create a secure channel between the Registration Offices and the certification system, as well as between this and the administrators/operators.

InfoCert's systems and networks are connected to the Internet in a controlled manner by a firewall system that allows for the connection to be split into gradually more secure areas: Internet network, DMZ (Demilitarised Zone) or Perimeter networks and Internal Networks. All the traffic that flows between the various areas is subject to acceptance by the firewall, based on a set of established rules. The rules defined on the firewalls are designed on the basis of "default deny" principles (what is not expressly permitted is forbidden by default, that is, the rules will only permit what is strictly necessary for the correct functioning of the application) and "defence in depth" (further levels of defence are organised, firstly at network level, via successive firewall barriers, and lastly the hardening at system level).

7 FORMAT

7.1 TSU certificate format

The information indicated in the certification request appears in the certificate. The produced certificate format complies with eIDAS Regulation and AgID Resolution n. 121/2019; this way full readability and verifiability is guaranteed in the context of the standards and European certifiers. InfoCert uses the ITU X.509 version 3 standard for the entire PKI structure.

7.1.1 Version number

All the certificates issued by InfoCert are X.509 version 3.

7.1.2 Certificate extensions

Qualified certificates are characterised by the extension found in the qcStatement clause 3.2.6 of IETF RFC 3739. Their use is governed by ETSI 319 412-2 and ETSI 319 422 standards.

7.1.3 Signature algorithm OID

The time stamp subscription algorithm. In this case, the algorithm used is the RSA. (Sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11);

7.1.4 Name forms

Each certificate contains an univocal serial number inside the TSA that issued it.

7.1.5 Name restrictions

See paragraph 3.1.

7.1.6 Certificate OID

See paragraph 1.2.

7.1.7 Time stamp format and content

The time stamp format and the TSA communication protocol comply with the technical specifications required in ETSI319422 [27]. Each time stamp issued contains all the information required by law, namely:

- The time stamp issuer's identification;
- The time stamp serial number;
- The certificate identification for the TSU public key;
- The time stamp generation date and time;
- The accuracy of the time source with respect to UTC. In this case it is a second or better;
- The identification of the hash algorithm used to generate the imprint of

computer evidence submitted to time stamping. In this case, the algorithm used is SHA-256 (secure hash algorithm 256-bit OID: 2.16.840.1.101.3.4.2.1);

- The value of the computer evidence imprint.

7.2 Stamp certificate CRL format

To create the lists of revoked CRLs, InfoCert uses the RFC5280 profile "Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)" and adds extensions as defined by RFC 5280 to the basic format: "Authority Key Identifier", "CRL Number ", "Issuing Distribution Point "and" expiredCertsOnCRL ".

7.2.1 Version number

All the certificates issued by InfoCert are X.509 version 2.

7.3 OCSP format

In order to be able to establish the certificate revocation status without making a request to the CRL, InfoCert makes OCSP services available that comply with the RFC6960 profile "X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol – OCSP". This protocol specifies the data that needs to be exchanged by an application that wishes to check the certificate status and OCSP service.

7.3.1 Version number

The OCSP protocol used by InfoCert complies with version 1 of the RFC6960.

8 COMPLIANCE AUDITS AND ASSESSMENTS

In order to obtain the qualification of qualified and unqualified trust service provider, in compliance with the eIDAS Regulation, it is essential to complete the process provided for under article 21 of the above mentioned Regulations.

InfoCert presented the specific request to AgID to obtain recognition as “qualified trust service provider” enclosing a conformity assessment report to the Regulation (Conformity Assessment Report - CAR) issued by an assessment body authorised by the national appointed body (CAB), which in Italy is ACCREDIA.

InfoCert offers the Service as qualified trust service provider under EU Regulations no. 910/2014 of 23/07/2014, on the basis of a conformity assessment carried out by the Conformity Assessment Body CSQA Certificazioni S.r.l., in compliance with the Regulation mentioned above and the ETSI EN 319 401 Standard, according to the eIDAS assessment scheme drawn up by ACCREDIA based on ETSI EN 319_403 and UNI CEI EN ISO/IEC 17065:2012 standards.

8.1 Conformity assessment frequency or circumstances

The conformity assessment is repeated every two years, but every year the CAB carries out a surveillance audit.

8.2 Identity/qualifications of assessor

Assessments are performed by

Company name	CSQA Certification S.r.l.
Registered office	Via S. Gaetano n. 74, 36016 Thiene (VI)
Telephone no.	+39 0445 313011
Registered with the Register of Companies under no.	Fiscal Code 02603680246 VI Business Register no. 02603680246/EAI no. 258305
VAT number	02603680246
Website	http://www.csqa.it

8.3 Relations between InfoCert and CAB

InfoCert and CSQA have no financial interests nor business relations.

There are no trade relations or partnerships that could create bias in favour of, or against InfoCert in CSQA's objective assessment.

8.4 Topics covered by assessment

The CAB is called upon to assess conformity with the CPS, the Guidelines and applicable standards of the procedures adopted, CA organisation, role organisation, staff training and contractual documents.

8.5 Actions taken in case of non conformity

In the event of non-compliance, the CAB will decide whether to send a report to the AgID or reserve the right to carry out another audit after the non-compliance has been rectified.

InfoCert aims to deal with all non-compliance aspects as quickly as possible, setting in motion all the actions required for improvement and adaptation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Time stamp issue fees

The fees are available from these sites <https://www.firma.infocert.it/> and <http://ecommerce.infocert.it>. The CA may enter into commercial agreements with specific fees.

9.1.2 Time stamp verification fees

Time stamp verification is free.

9.1.3 Fees for other services

The fees are available from these sites <https://www.firma.infocert.it/> and <http://ecommerce.infocert.it>. The CA may enter into commercial agreements with specific fees.

9.1.4 Refund policies

Should the service be purchased by a consumer, the Subject has the right to withdraw from the contract within 14 days from the date the contract was concluded, obtaining a reimbursement on the price paid. The instructions for exercising the right of withdrawal and the request for a reimbursement are available from the website <https://help.infocert.it/>

9.2 Financial responsibilities

9.2.1 Insurance cover

InfoCert TSP has stipulated an insurance contract covering risks during work and damage caused to third parties, whose text was negotiated and accepted by AgID which as coverage limit has:

- 10.000.000 Euro for a single accident;
- 10.000.000 Euro per year.

9.2.2 Warranty and insurance cover for end subjects

See paragraph 9.2.1.

9.3 Business information confidentiality

9.3.1 Area of application of confidential information

Confidential information management is not part of the activities mentioned in this Manual.

9.4 Privacy

Save as expressly permitted, any Subject's/Subscriber's information acquired by the CA while performing its routine activities shall be regarded as confidential and non-disclosable, except for information specifically intended for public use [e.g. public key, certificates (if requested by the Subject), certificate revocation and suspension dates]. In particular, personal data shall be processed by the Certification Authority in accordance with Legislative Decree No. 196 of 30 June 2003[4] and with European Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection of natural persons with regard to the processing of personal data and on the free movement of such data, fully binding starting from 25 May 2018 [4].

9.4.1 Privacy plan

InfoCert adopts a set of policies through which it implements and integrates personal data protection within its ISO 27001 certified Information Security Management System, sharing the continuous improvement process with this system.

9.4.2 Information treated as private

Data that falls under the corresponding definition found in the current law [4] is considered personal; personal data refers to any information regarding the physical person, identified or identifiable, even indirectly, via reference to any other information, including a personal identification number.

9.4.3 Processing of personal data

InfoCert S.p.A.

Operating Headquarters

Via Marco e Marcelliano, 45

00147 Rome

richieste.privacy@legalmail.it

9.4.4 Privacy information and personal data processing consent

The privacy information sheet can be found on the website www.infocert.it.

Before processing any personal data, InfoCert shall obtain consent to the processing in compliance with the law [4].

9.4.5 Data disclosure following requests from the authorities

Data disclosure on request from the Authorities is obligatory and follows the instructions established by the Authorities themselves case by case.

9.4.6 Other disclosure reasons

Not foreseen.

9.5 Intellectual property rights

The copyright in this document belongs to InfoCert SpA. All rights reserved.

9.6 Representation and warranty

InfoCert retains responsibility for complying with the procedures prescribed in its information security policy, including when certain functions are delegated to a third party.

The Client or the Applicant is responsible for the truthfulness of the data communicated to the Certification Authority. The Client or the Applicant is also obliged to let know as well as to obtain acceptance of the general time stamp validation service conditions and of the present Practice statement by all the subjects that use the service.

9.7 Warranty limitation

The Certification Authority does not provide any warranties on (i) the proper operativity and safety of hardware and software used by the Applicant; (ii) the use of time stamp different from those provided by current regulations and this Practice Statement; (iii) the continuity of national and/or international electricity and telephone lines; (iv) the validity and relevance, including probatory, of the any message, deed or document associated with the time stamp.

The Certification Authority only guarantees the operating of the Service, according to the levels specified in paragraph 9.18 of the present Practice Statement.

9.8 Liability limitation

The service is provided in accordance to the contract for the Time Stamp Services (hereinafter also the referred to as the "Contract"). The Certification Authority does not carry out any verification of the document for which the Time Stamp is requested, as such determinations and information are known and sent directly by the Applicant under his own and exclusive liability.

The Certification Authority does not undertake any obligation to monitor the content, the type or the electronic format of the documents and possibly of the hash sent by the IT procedure indicated by the Applicant or the Owner, so not having liability, unless wilful misconduct or negligence with reference to the validity and imputability of them to the actual intention of the Applicant.

Except in case of wilful misconduct or gross negligence, the Certification Authority shall not be liable for any direct or indirect damage suffered by the Owners and/or by third parties because of the use or non-use of the time stamp certificates issued in accordance with the provisions of this Statement and the General Conditions of the Time Stamp Services.

InfoCert is not responsible for any direct and/or indirect damage deriving, also alternatively, from: i) loss, ii) improper storage, iii) improper use of time stamp tools and/or failure of the Applicant in complying with the recommendations mentioned above.

Moreover, also from the phase of formation of the Contract as well as during its execution, the Certification Authority is not liable for any damages and/or delays due to malfunctioning or arrest of the computer system and internet.

Except in the case of wilful misconduct or gross negligence, InfoCert shall not be burdened with charges or liability for direct or indirect damages of any nature or importance that may occur to the Applicant and/or to third parties caused by third parties unauthorized by InfoCert tampering or interfering with the service or equipment.

9.9 Indemnity

InfoCert is responsible for possible damages directly determined, intentionally or by negligence, to any natural or legal person, as a result of failure to comply with the obligations set out in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 and by InfoCert's failure to use all the appropriate measures to avoid the damage.

In such case the Applicant or the Owner will have the right to obtain, as compensation for the damages directly suffered as a result of the behavior referred to in the previous paragraph, an amount that can not in any case exceed the maximum values envisaged, for each claim and per year, by art. 3, c. 7, of the Regulation attached to the Determination 185/2017.

The refund may not be requested if the failure to use the service is due to the misuse of the certification service or to the telecommunication network operator or to incidental events, force majeure or causes not attributable to InfoCert such as, for example, strikes, revolts, earthquakes, acts of terrorism, popular riots, organised sabotage, chemical and/or bacteriological events, war, floods, measures put in place by competent authorities or to inadequacy of structures, hardware and/or software used by the Applicant.

9.10 Term and termination

9.10.1 Term

The effects of the Contract are produced starting from its conclusion and persist until the last Time Stamp purchased with a single purchase order is used.

The duration of the Time Stamp Service Contract is equal to the duration of the Time Stamp.

In case of termination of the Contract, for any reason it occurs, it will no longer be possible to use the Service.

9.10.2 Termination

The Contract automatically terminates according to law, with consequent interruption of the Service and revocation of time stamp credentials, if the Applicant does not fulfil the contract provisions foreseen in art. 1 (subject of the contract, specifications of the service and relationships between the parties), art. 6 (considerations), art. 7 (Identifier and access to the system); art. 11.1. (Obligations of the Applicant), art. 11.2 (Liability of the Applicant) as well as the provisions of the present Practice Statement or in case of untrue declarations made by the Applicant for the Contract or for the issuing of the Time Stamp. Termination will occur according to law, if the interested party communicates to the other party via PEC or registered letter with acknowledgement of receipt to make use of the present clause.

In all the cases the obligations are not fulfilled by the Applicant, InfoCert will be entitled to suspend the fruition of the service, by suspending the time stamp credentials.

In case of opening of an insolvency or other insolvency proceedings by one of the party, the other party shall be entitled to terminate the Contract as well as all other relationships with the other party, without any notice period and any liability. In any case of cancellation, cessation, withdrawal or termination of the Contract, for any reason it occurs, the consideration foreseen by the above-mentioned art. 6 is still due and, if already paid, shall not be refunded.

This without prejudice to the compensation for any further damage suffered by InfoCert in case of breach of the Contract by the Applicant.

In case the Applicant is a consumer, provisions of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights apply. Civil disputes related to the Contract with the consumer are subject to the mandatory territorial jurisdiction of the court of the consumer's place of residence or domicile.

Although InfoCert has no obligation to use any alternative dispute resolution entity, the consumer is informed about the possibility too make use, on a voluntary basis, of the extra judicial dispute resolution methods provided for by applicable law.

It should also be noted that, pursuant to EU Regulation no. 524/2013, about the resolution of disputes relating to online contracts and services offered online, there is the possibility of resorting to the Online Dispute Resolution (ODR) procedure, provided by the European Commission and available at the following link: <https://webgate.ec.europa.eu/odr/>.

9.10.3 Termination effects

Termination implies the immediate impossibility of using the time stamping service.

9.11 Official communication channels

Please consult the contact channels found in paragraph 1.5.

9.12 Amendments

The CA reserves the right to make changes to this document for technical purposes as well as changes to procedures required due to both laws or regulations and to maximise the work cycle. Each new version of the CPS voids and replaces the previous versions that remain, however, applicable to certificates issued during their validity and up until their first expiry date.

Variations that have not had a significant impact on users leads to the increase in the document release number, while variations with a significant impact on users (such as, for example, changes regarding operating procedures) lead to an increase in the document version number. In any case, the manual will be immediately published and made available following the methods provided. Any technical or procedural change to this document shall be immediately communicated to the RA.

If the changes are relevant, the CA must undergo an audit by an accredited CAB, submit the certification report (*CAR - Conformity Assessment Report*) and the CPS to the Supervisory Bodies (AgID) and wait for permission to publish.

9.12.1 Revision history

Versione/Release no:	2.8
Version/Release date:	13/05/2022
Change description:	<p>§ 5 Added detail on frequency of security policy review §§ 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.6, 5.5.1, 5.5.2, 5.5.3, 5.5.5, 5.5.6, 5.5.7 Specification of storage methods § 5.5.6 Update of detail of the procedure</p> <p>Formatting for document accessibility</p>
Reasons:	<p>General review Edit formatting</p>

Version/Release no:	2.7
Version/Release date:	16/09/2021
Change description:	§ 1.5.1: change of contact information
Reasons:	Contact information update

Version/Release no:	2.6
Version/Release date:	15/06/2021
Change description:	<p>Change to the title of the document with the addition of the not qualified timestamp service</p> <p>§ 1.1: Addition of the not qualified service</p> <p>§ 1.2: Added not qualified policies and revised description</p> <p>§ 1.4.1: Change of name of verification software</p> <p>§ 5.3.5: Update description of work shifts</p> <p>§ 5.8: Description review</p> <p>§ 4.9: Clarification regarding information on the revocation status</p> <p>§ 5.1.1: Technological update</p> <p>§ 5.7.3: Description update</p> <p>§ Annex A: Added annex with TSA root certificates</p> <p>Spelling corrections</p>
Reasons:	<p>New roots</p> <p>Periodic review</p>

Version/Release no:	2.5
Version/Release date:	22/05/2020
Change description:	<p>§ 5.1.1 Technological update</p> <p>§ 5.1.6 Technological updating of storage media</p>
Reasons:	Technological update

Version/Release no:	2.4
Version/Release date:	03/12/2019
Change description:	§ 1.2 OID AgIDcert introduction § 5.1.1 Datacenter location § 5.3.7 physical and logical access § 5.4.1 added physical and logical log description
Reasons:	Typo correction Agid Resolution n. 121/2019 come into effect

Version/Release no:	2.3
Version/Release date:	30/11/2018
Change description:	§ 1.3 Group named changed in "tinexta"
Reasons:	Name of the group changed

Version/Release no:	2.2
Version/Release date:	19/06/2018
Change description:	§ 1.5, § 9.2, § 9.4, § 9.15 New phone contacts, Insurance cover, privacy, Typo correction, document code.
Reasons:	

Version/Release no:	2.1
Version/Release date:	09/04/2018
Change description:	Typo correction § 9.6, § 9.7, § 9.8, § 9.9, § 9.10 rewriting of these par. for a better contextualization
Reasons:	

Version/Release no.:	2.0.1
Version/Release Date:	28/07/2017
Change description:	Corrected minus mistakes in \$4.3 and \$4.7
Reasons:	-

Version/Release no.:	2.0
Version/Release Date:	02/05/2017
Change description:	Relocated content on RFC 3647 index
Reasons:	-

Version/Release no.:	1.0
Version/Release Date:	01/07/2016
Change description:	First issue
Reasons:	-

9.12.2 Revision procedures

The certificate practice statement revision procedures are the same as the drafting procedures. This revisions are made jointly with the Certification Service Manager, the Security Manager, the Privacy Manager, the Legal Department and the Consulting Area, and approved by management.

9.12.3 Notification period and mechanism

The CPS is published:

- in electronic format on the TSP website (address: <http://www.firma.infocert.it/doc/manuali.htm>);
- in electronic format in the public list of certifiers held by AgID.

9.13 Disputes

Please consult the contract governing the service for details of dispute resolution methods.

9.14 Jurisdiction

For consumers, jurisdiction shall be in the city where the consumer resides. For those other than consumers, jurisdiction shall be in Rome. In the agreements between CA and Subject, a different jurisdiction may be defined.

9.15 Applicable law

The law governing this document is Italian law.

The following is a complete list of the main applicable reference laws:

- [1] EU Regulation no. 910/2014 of the European Parliament and Council dated 23 July 2014 governing electronic identification and trust service for electronic transactions in the internal market and that repeals Directive 1999/93/EC (also referred to as *eIDAS Regulation*).
- [2] Italian Legislative Decree no. 82 dated 7 March 2005, (OJ no. 112 of 16 May 2005) – Digital administration Code (also referred to as *CAD*) as amended.
- [3] *not used*
- [4] Italian Legislative Decree no. 196 of 30 June 2003, (OJ no. 174 of 29 July 2003) – Privacy Code as amended and regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (in force starting from 25 Mai 2018)
- [5] *not used*
- [6] *not used*
- [7] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights and related national transposing legislation
- [8] Preliminary verification – 24 September 2015 [4367555] Processing personal data in the context of the ‘Emission process by webcam recognition’ for qualified or digital electronic signature.
- [9] CNIPA ("The National Centre for IT in the Public Administration") Decision no. 45 of 21 May 2009, as amended by subsequent resolutions.
- [10] Resolution AgID no. 189/2017
- [11] Furthermore, all the circulars and resolutions from the Supervisory Authorities¹, as well as the implementation acts provided for under the eIDAS Regulation [1] apply.

¹ Available on website <http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche>

[12] AgID Resolution n.121/2019 ver 1.1 (in place of CNIPA Resolution 45/2009).

9.16 Reference standards

Below is a non-exhaustive list of reference standards applicable to the service:

- i. ETSI EN 319 401 V2.1.1 - ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); GENERAL POLICY REQUIREMENTS FOR TRUST SERVICE PROVIDERS;
- ii. ETSI EN 319 421 V1.1.1 -ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); POLICY AND SECURITY REQUIREMENTS FOR TRUST SERVICE PROVIDERS ISSUING TIME-STAMPS, hereinafter ETSI319421;
- iii. ETSI EN 319 422 V1.1.1 (2016-03) ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); TIME-STAMPING PROTOCOL AND TIME-STAMP TOKEN PROFILES, hereinafter ETSI319422.

9.17 Various regulations

Please consult the contract governing the service for any other regulation not found in this Manual.

9.18 Other provisions

The service provision times are (unless otherwise agreed in the contract):

Service	Hours
Time stamp request	From 0:00 to 24:00 24/7
Time stamp verification	From 0:00 to 24:00 24/7

Annex A

Time stamp root "InfoCert Time Stamping Authority 2"

```
0 1266: SEQUENCE {
4 986: SEQUENCE {
8 3: [0] {
10 1: INTEGER 2
: }
13 1: INTEGER 3
16 13: SEQUENCE {
18 9: OBJECT IDENTIFIER
: sha256WithRSAEncryption (1 2 840 113549 1 1 11)
29 0: NULL
: }
31 117: SEQUENCE {
33 11: SET {
35 9: SEQUENCE {
37 3: OBJECT IDENTIFIER countryName (2 5 4 6)
42 2: PrintableString 'IT'
: }
: }
46 21: SET {
48 19: SEQUENCE {
50 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
55 12: UTF8String 'INFOCERT SPA'
: }
: }
69 12: SET {
71 10: SEQUENCE {
73 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
78 3: UTF8String 'TSA'
: }
: }
83 20: SET {
85 18: SEQUENCE {
87 3: OBJECT IDENTIFIER serialNumber (2 5 4 5)
92 11: PrintableString '07945211006'
: }
: }
105 43: SET {
107 41: SEQUENCE {
109 3: OBJECT IDENTIFIER commonName (2 5 4 3)
114 34: UTF8String 'InfoCert Time Stamping Authority 2'
: }
: }
: }
150 30: SEQUENCE {
152 13: UTCTime 19/04/2013 14:30:33 GMT
167 13: UTCTime 19/04/2029 15:30:33 GMT
: }
182 117: SEQUENCE {
184 11: SET {
186 9: SEQUENCE {
188 3: OBJECT IDENTIFIER countryName (2 5 4 6)
193 2: PrintableString 'IT'
: }
: }
197 21: SET {
199 19: SEQUENCE {
201 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
```



```

206 12:    UTF8String 'INFOCERT SPA'
      :    }
      :    }
220 12:    SET {
222 10:    SEQUENCE {
224 3:     OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
229 3:     UTF8String 'TSA'
      :     }
      :     }
234 20:    SET {
236 18:    SEQUENCE {
238 3:     OBJECT IDENTIFIER serialNumber (2 5 4 5)
243 11:    PrintableString '07945211006'
      :    }
      :    }
256 43:    SET {
258 41:    SEQUENCE {
260 3:     OBJECT IDENTIFIER commonName (2 5 4 3)
265 34:    UTF8String 'InfoCert Time Stamping Authority 2'
      :     }
      :     }
      :     }
301 290:   SEQUENCE {
305 13:    SEQUENCE {
307 9:     OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
318 0:     NULL
      :     }
320 271:   BIT STRING, encapsulates {
325 266:   SEQUENCE {
329 257:   INTEGER
      :     00 C1 82 81 37 2D 2F 2A A4 48 26 15 AE 06 D6 87
      :     E2 45 EA 4C 39 0C 4B 6C 35 DE AB 35 8C B8 74 3C
      :     67 BE 75 28 7F 94 1A 48 20 A0 1F 33 14 88 FA D3
      :     8A 65 9A 8B CC 53 A2 AC F3 E3 69 D4 AC 7F 67 D6
      :     77 33 90 36 5E F9 87 30 4D 6E 5C F9 A9 F0 AB 8D
      :     86 91 17 B7 82 0B 34 EE E7 8C CD 6F CB FF 84 DC
      :     CF 74 EA B0 E1 1C 60 86 CF 51 15 9C 87 96 45 FB
      :     54 28 14 C6 8E F3 B1 CE C4 2C BD 0B 81 A0 D9 64
      :     2A 11 79 0A FE 81 89 ED 0C 9C 7E 4C ED EE BA 8B
      :     C5 07 FC CE B2 C6 B0 C6 13 67 C3 EE 08 87 F8 99
      :     F9 80 3A 54 14 A1 18 D8 C9 3F 9A 1B 7F 82 C7 F0
      :     7D 33 3B F9 25 54 FB 36 14 40 0B C2 B2 0E BE 7D
      :     55 82 96 AE 71 D5 8B 88 E4 F6 3D 5C 2B 87 EC 6E
      :     72 4D BD F4 7D 57 BC C1 6A EF D1 E6 95 05 F3 CA
      :     4A CF 17 64 2C 0B 5C AD AF 26 F3 46 D2 C8 1F 20
      :     5B 9C 48 96 80 F2 2C FB A1 8E 8B 56 C7 DF 62 99
      :     3F
590 3:    INTEGER 65537
      :    }
      :    }
      :    }
595 395:   [3] {
599 391:   SEQUENCE {
603 15:    SEQUENCE {
605 3:     OBJECT IDENTIFIER basicConstraints (2 5 29 19)
610 1:     BOOLEAN TRUE
613 5:     OCTET STRING, encapsulates {
615 3:     SEQUENCE {
617 1:     BOOLEAN TRUE
      :     }
      :     }
      :     }
620 88:    SEQUENCE {
622 3:     OBJECT IDENTIFIER certificatePolicies (2 5 29 32)

```

```

627 81:    OCTET STRING, encapsulates {
629 79:    SEQUENCE {
631 77:    SEQUENCE {
633 4:     OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
639 69:    SEQUENCE {
641 67:    SEQUENCE {
643 8:     OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
653 55:    IA5String
      :    'http://www.firma.infocert.it/documentazione/manu'
      :    'ali.php'
      :    }
      :    }
      :    }
      :    }
      :    }
710 37:    SEQUENCE {
712 3:     OBJECT IDENTIFIER issuerAltName (2 5 29 18)
717 30:    OCTET STRING, encapsulates {
719 28:    SEQUENCE {
721 26:    [1] 'firma.digitale@infocert.it'
      :    }
      :    }
      :    }
749 195:   SEQUENCE {
752 3:     OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
757 187:   OCTET STRING, encapsulates {
760 184:   SEQUENCE {
763 181:   SEQUENCE {
766 178:   [0] {
769 175:   [0] {
772 40:   [6] 'http://crl.infocert.it/crls/tss2/ARL.crl'
814 130:   [6]
      :    'ldap://ldap.infocert.it/cn%3DInfoCert%20Time%20S'
      :    'tamping%20Authority%202,ou%3DTSA,o%3DINFOCERT%20'
      :    'SPA,C%3DIT?authorityRevocationList'
      :    }
      :    }
      :    }
      :    }
      :    }
947 14:    SEQUENCE {
949 3:     OBJECT IDENTIFIER keyUsage (2 5 29 15)
954 1:     BOOLEAN TRUE
957 4:     OCTET STRING, encapsulates {
959 2:     BIT STRING 1 unused bit
      :     '1100000'B
      :     }
      :     }
963 29:    SEQUENCE {
965 3:     OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
970 22:    OCTET STRING, encapsulates {
972 20:    OCTET STRING
      :    07 36 16 18 B5 0E FD 77 8F 5D 68 25 F2 38 FD 6F
      :    34 26 F5 F7
      :    }
      :    }
      :    }
      :    }
994 13:    SEQUENCE {
996 9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1007 0:    NULL
  
```

```

: }
1009 257: BIT STRING
: 4E CB 99 48 10 A8 8F 80 68 80 D4 C5 FE EE F7 E0
: 42 3E 65 AB B8 A7 84 18 F5 B1 7B 2B 66 C7 E7 6C
: 60 0F E1 91 3D D4 7D 25 02 80 5F 1E 36 A6 F0 1E
: 91 54 D9 C2 7F 32 01 80 5B D4 29 57 58 5E 1B BE
: F3 C9 98 B2 55 87 DB 17 CB 4D B9 F0 8F 7C F3 D9
: 34 FF 73 EB EA 14 3D 9E E1 7E 7E 7C 42 08 05 C3
: B0 A8 11 D2 D6 C9 1D 80 59 74 24 A9 0B FC 5B 45
: 4D 1B 4E 6D 27 61 3C E4 42 45 D9 BE FF 28 7E 25
: 0C 65 D4 D8 45 9D 76 5F 09 D5 22 8F 50 5C 84 B3
: A7 3D 78 20 DD 98 1E F1 79 59 A0 A4 C7 36 F2 A9
: B2 F0 3B 2D 9D 4D E1 EB F8 21 7B 9D 60 B0 CF 64
: 21 A2 C7 C3 FA 05 1F AA 7B 08 DA DA 7C 2C 75 63
: 9A 16 83 F1 77 7D 8B B5 E0 85 DB 33 CA B0 22 54
: 46 42 2C E1 86 F2 28 A2 53 3A 99 13 65 66 CA D5
: 47 47 34 88 F8 1C 75 68 EE 65 68 F9 57 38 B2 A1
: 76 BC FD 87 15 37 B4 EB B8 56 A5 BF AF 53 46 48
: }
    
```

Qualified time stamp root "Qualified InfoCert Time Stamping Authority 2"

```

0 1810: SEQUENCE {
4 1274: SEQUENCE {
8 3: [0] {
10 1: INTEGER 2
: }
13 1: INTEGER 1
16 13: SEQUENCE {
18 9: OBJECT IDENTIFIER
: sha256WithRSAEncryption (1 2 840 113549 1 1 11)
29 0: NULL
: }
31 127: SEQUENCE {
33 11: SET {
35 9: SEQUENCE {
37 3: OBJECT IDENTIFIER countryName (2 5 4 6)
42 2: PrintableString 'IT'
: }
: }
46 21: SET {
48 19: SEQUENCE {
50 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
55 12: UTF8String 'INFOCERT SPA'
: }
: }
69 12: SET {
71 10: SEQUENCE {
73 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
78 3: UTF8String 'TSA'
: }
: }
83 20: SET {
85 18: SEQUENCE {
87 3: OBJECT IDENTIFIER serialNumber (2 5 4 5)
92 11: PrintableString '07945211006'
: }
: }
105 53: SET {
107 51: SEQUENCE {
109 3: OBJECT IDENTIFIER commonName (2 5 4 3)
114 44: UTF8String
: 'InfoCert Qualified Time Stamping Authority 2'
    
```

```

:   }
:   }
:   }
160 30: SEQUENCE {
162 13:   UTCTime 28/06/2016 14:18:40 GMT
177 13:   UTCTime 28/06/2026 15:18:40 GMT
:   }
192 127: SEQUENCE {
194 11:   SET {
196 9:    SEQUENCE {
198 3:    OBJECT IDENTIFIER countryName (2 5 4 6)
203 2:    PrintableString 'IT'
:    }
:   }
207 21: SET {
209 19: SEQUENCE {
211 3:  OBJECT IDENTIFIER organizationName (2 5 4 10)
216 12: UTF8String 'INFOCERT SPA'
:   }
:   }
230 12: SET {
232 10: SEQUENCE {
234 3:  OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
239 3:  UTF8String 'TSA'
:   }
:   }
244 20: SET {
246 18: SEQUENCE {
248 3:  OBJECT IDENTIFIER serialNumber (2 5 4 5)
253 11: PrintableString '07945211006'
:   }
:   }
266 53: SET {
268 51: SEQUENCE {
270 3:  OBJECT IDENTIFIER commonName (2 5 4 3)
275 44: UTF8String
:   'InfoCert Qualified Time Stamping Authority 2'
:   }
:   }
:   }
321 546: SEQUENCE {
325 13: SEQUENCE {
327 9:  OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
338 0:  NULL
:   }
340 527: BIT STRING, encapsulates {
345 522: SEQUENCE {
349 513: INTEGER
:   00 9F AB C7 3F 53 A6 89 34 EF 57 D7 FA 95 51 7A
:   13 40 B9 99 25 1C BA 39 6E 8C 70 CD 49 5E 66 D4
:   5D EC 6C 82 2F F7 B2 16 87 D3 ED BF 07 CF 58 5B
:   0C A8 EC 5C 8C CE E9 D6 14 7A 52 F9 72 5F 4B C8
:   16 7E 5C CE 78 06 10 88 0A C8 8C 24 B4 60 A8 2D
:   7D 3D 0A AA 83 50 FA F5 CA 9A 91 C9 56 A6 D8 66
:   61 C9 46 46 89 50 07 2F 52 73 70 8C 54 F8 84 6B
:   C5 19 DC 7B B4 69 3B 6B 37 52 2F E0 F3 5C 8D 06
:   CB F8 E7 7E A6 36 69 27 8C 04 EA 3C CD 2E A7 2D
:   31 7B 6D E8 9D 41 2B DA F4 F9 07 98 31 FB BA B1
:   88 20 17 B7 3F 9A 57 09 3F F6 AD 6C CC 7F 3A 41
:   EE 72 E1 AF E0 8D 74 5F 0F 66 29 21 9C 4F C9 43
:   19 2B 77 4F A7 F7 61 3D 9B 25 B5 E9 33 81 F7 A8
:   1F AD 11 7E 3D E4 E9 44 99 05 13 57 34 B0 A2 45
:   58 FD 8D 0F 37 70 7D C4 BD F3 D7 B6 E5 7C 1C 8F
:   AE 26 2A AF E8 17 CC 46 EC 50 A5 DC 62 59 BA 54

```

```

:      2F D9 B3 E1 9F A3 5C D5 CE 80 DE 5D 37 F6 7E BD
:      E0 8D 2D 9C 3F C0 1E 0F DA B0 23 EE 5D B7 71 11
:      0C EB 87 E7 2E 48 61 71 FF B5 FE 83 69 DB 4F E2
:      7D 86 B3 46 A3 11 FD 1E 38 BC 1B 03 70 E1 2A E0
:      73 BD 05 45 C7 7E 87 BC 46 0F AE BA C7 5E B1 76
:      08 32 62 1A 7E 8F 6D EE 71 82 CB 3E B6 FA 61 E8
:      56 21 32 0F 86 58 96 F2 C7 DC 83 6B C7 81 E5 CE
:      29 CE AA A6 20 63 8F C3 78 A3 F6 5E 8B 41 62 B0
:      A4 CF 49 5B D3 ED EA A0 97 3B D5 D0 82 99 F2 48
:      39 CE 8B 82 22 B8 DC 78 27 E1 A2 74 14 8E 18 B2
:      E4 F0 CE FA 19 AA 40 A8 0A 44 AC E3 79 F4 99 53
:      0E C8 23 29 BB 80 71 7D 8B 0E AF B7 B5 A7 17 F7
:      8A E2 53 19 AC 71 86 0A BE 46 26 FC 22 62 8A A7
:      4E 08 25 3F D5 19 20 39 1E ED 0B D2 4D 38 8E 1A
:      15 5B F5 D1 C7 AC BE DE 04 7D D5 8E EE 89 63 51
:      B6 33 FA ED 6A 57 CB 7B B9 F1 38 B2 39 B4 8D CD
:      FF
866 3:  INTEGER 65537
:      }
:      }
:      }
871 407: [3] {
875 403:  SEQUENCE {
879 15:   SEQUENCE {
881 3:    OBJECT IDENTIFIER basicConstraints (2 5 29 19)
886 1:    BOOLEAN TRUE
889 5:    OCTET STRING, encapsulates {
891 3:      SEQUENCE {
893 1:        BOOLEAN TRUE
:      }
:    }
:  }
896 88:  SEQUENCE {
898 3:    OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
903 81:  OCTET STRING, encapsulates {
905 79:  SEQUENCE {
907 77:  SEQUENCE {
909 4:    OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
915 69:  SEQUENCE {
917 67:  SEQUENCE {
919 8:    OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
929 55:  IA5String
:      'http://www.firma.infocert.it/documentazione/manu'
:      'ali.php'
:    }
:  }
:  }
:  }
:  }
:  }
986 37:  SEQUENCE {
988 3:    OBJECT IDENTIFIER issuerAltName (2 5 29 18)
993 30:  OCTET STRING, encapsulates {
995 28:  SEQUENCE {
997 26:    [1] 'firma.digitale@infocert.it'
:    }
:  }
:  }
1025 207: SEQUENCE {
1028 3:   OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1033 199: OCTET STRING, encapsulates {
1036 196: SEQUENCE {
1039 193: SEQUENCE {
1042 190: [0] {

```

```

1045 187:      [0] {
1048 40:      [6] 'http://crl.infocert.it/crls/qtss/ARL.crl'
1090 142:      [6]
:      'ldap://ldap.infocert.it/cn%3DInfoCert%20Qualifie'
:      'd%20Time%20Stamping%20Authority%202,ou%3DTSA,o%3'
:      'DINFOCERT%20SPA,c%3DIT?authorityRevocationList'
:      }
:      }
:      }
:      }
:      }
:      }
1235 14:      SEQUENCE {
1237 3:      OBJECT IDENTIFIER keyUsage (2 5 29 15)
1242 1:      BOOLEAN TRUE
1245 4:      OCTET STRING, encapsulates {
1247 2:      BIT STRING 1 unused bit
:      '1100000'B
:      }
:      }
1251 29:      SEQUENCE {
1253 3:      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1258 22:      OCTET STRING, encapsulates {
1260 20:      OCTET STRING
:      AE 92 81 E5 30 55 6D C8 4A 74 78 A1 71 6D 3F 39
:      02 FE 58 87
:      }
:      }
:      }
:      }
1282 13:      SEQUENCE {
1284 9:      OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1295 0:      NULL
:      }
1297 513:      BIT STRING
:      39 46 9B E9 7A 02 72 D5 F8 11 D4 94 42 80 26 CE
:      2F DD 56 82 92 D5 68 05 14 D2 F0 C8 0C 5B 11 CF
:      88 F0 94 3D 66 B9 B8 52 35 B1 E5 A1 9C 83 2C F3
:      5B 4E AA 2E D8 B1 75 61 E0 FB 96 86 0C EC AB F6
:      2A A8 5B 61 C7 20 46 32 48 75 01 52 23 09 7E 7D
:      88 41 B5 80 0D 0B 0F 8F 63 7F D5 4B 25 58 7A D3
:      4A 5C 1C DA B2 83 5F BF B5 CB 9F 73 08 BD 17 84
:      57 5F 8E 6D 9B 15 6F 21 03 8A 9C 3E 94 03 34 D9
:      A4 08 62 08 03 39 38 9B F6 1B C6 D3 FB 1D BD DE
:      23 E9 FA F5 62 73 2E EC 1E 9B 18 40 24 BE 45 8B
:      E8 A6 F6 79 FC EB 98 60 C7 9D 85 E6 C8 4C CC AB
:      14 10 2A 50 AD 96 90 76 A9 82 BB D1 F9 91 48 1B
:      B5 5B A5 E7 6B D3 C8 E6 D4 C8 9A 44 30 9F E1 DF
:      C2 B5 6F ED 7D E7 E6 3C 01 07 BA 28 DA E4 06 E0
:      04 22 6F 50 0F 58 74 A3 F1 71 B2 CD 74 68 27 73
:      CF 14 31 91 F8 14 F5 13 E0 6A ED 00 7D D6 10 D8
:      69 94 99 37 DD A4 B1 83 41 46 75 9C BC 7D 7F 2C
:      A5 E3 46 6E AC C9 AE 75 87 F0 FD AC C5 52 12 EC
:      F3 FB 89 78 00 E7 C7 40 C6 59 98 F5 FA 15 6D 79
:      8D AE 88 4A 60 F9 E3 61 6C 20 0A 48 61 7D D0 69
:      4B 9E 27 A7 0E 81 2D 12 FB 12 78 11 4A EF 96 B5
:      6D D4 E1 D1 4C 46 15 25 70 E6 BA 07 45 62 0C 8C
:      77 D0 67 5D 07 6C 1C A3 59 4F E5 FE A3 F0 DF 8C
:      D5 9A BA 30 B5 35 8E 36 10 DA 20 7C E4 69 EA 17
:      2C A4 72 32 E0 D4 30 92 DF B3 79 41 F1 C9 83 DC
:      90 DF 69 4A 14 39 2F CE 7D CE 1A 03 62 7A 82 0D
:      79 A5 BD FC 69 25 9D 05 71 97 1D A3 C3 BF 06 EF
:      EE 1D E5 2F BE CB 26 AC 7A 84 2F 1F AF D1 5A D9

```

```

: 4A CC 97 11 70 27 4F 35 78 1E 74 10 8C AD 58 A9
: 54 8D 6A 05 B0 5C 51 A6 6E 5F 5D 40 5A 25 53 CD
: 7A EF 82 F4 FC 89 06 5C 0E CE BA 2C 18 B2 7F 90
: D3 0C AF 56 B1 17 15 47 6A DA 40 3D 3E 32 EA D4
: }

```

Time stamp root "InfoCert Time Stamping Authority 3"

```

0 1755: SEQUENCE {
4 1219: SEQUENCE {
8 3: [0] {
10 1: INTEGER 2
: }
13 1: INTEGER 1
16 13: SEQUENCE {
18 9: OBJECT IDENTIFIER
: sha256WithRSAEncryption (1 2 840 113549 1 1 11)
29 0: NULL
: }
31 126: SEQUENCE {
33 11: SET {
35 9: SEQUENCE {
37 3: OBJECT IDENTIFIER countryName (2 5 4 6)
42 2: PrintableString 'IT'
: }
: }
46 24: SET {
48 22: SEQUENCE {
50 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
55 15: UTF8String 'InfoCert S.p.A.'
: }
: }
72 12: SET {
74 10: SEQUENCE {
76 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
81 3: UTF8String 'TSA'
: }
: }
86 26: SET {
88 24: SEQUENCE {
90 3: OBJECT IDENTIFIER '2 5 4 97'
95 17: UTF8String 'VATIT-07945211006'
: }
: }
114 43: SET {
116 41: SEQUENCE {
118 3: OBJECT IDENTIFIER commonName (2 5 4 3)
123 34: UTF8String 'InfoCert Time Stamping Authority 3'
: }
: }
159 30: SEQUENCE {
161 13: UTCTime 07/06/2021 08:19:06 GMT
176 13: UTCTime 07/06/2033 09:19:06 GMT
: }
191 126: SEQUENCE {
193 11: SET {
195 9: SEQUENCE {
197 3: OBJECT IDENTIFIER countryName (2 5 4 6)
202 2: PrintableString 'IT'
: }
: }
206 24: SET {
208 22: SEQUENCE {

```

```

210 3:    OBJECT IDENTIFIER organizationName (2 5 4 10)
215 15:   UTF8String 'InfoCert S.p.A.'
      :   }
      :   }
232 12:   SET {
234 10:   SEQUENCE {
236 3:    OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
241 3:    UTF8String 'TSA'
      :    }
      :    }
246 26:   SET {
248 24:   SEQUENCE {
250 3:    OBJECT IDENTIFIER '2 5 4 97'
255 17:   UTF8String 'VATIT-07945211006'
      :   }
      :   }
274 43:   SET {
276 41:   SEQUENCE {
278 3:    OBJECT IDENTIFIER commonName (2 5 4 3)
283 34:   UTF8String 'InfoCert Time Stamping Authority 3'
      :   }
      :   }
319 546:  SEQUENCE {
323 13:   SEQUENCE {
325 9:    OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
336 0:    NULL
      :    }
338 527:  BIT STRING, encapsulates {
343 522:  SEQUENCE {
347 513:  INTEGER
      :    00 E2 74 6C AF FB 6F 8E 1C AF C0 BF 47 F6 6B F9
      :    0A B2 58 C9 13 38 EC 92 5C B1 5C 48 2C 45 47 5E
      :    8A 2C 52 D7 E0 19 D7 BC F8 C6 F2 97 C8 2A B6 76
      :    8C 22 3C CD 75 9D E7 2E D2 8B E7 61 8C 63 71 A2
      :    2C DE B3 0C B7 ED 0D 3B C1 8A 87 CC 64 9B 05 07
      :    BA 06 1A 17 19 AC C6 DD 8E D0 B3 2B B5 CD 0A C7
      :    18 89 AA 3C 21 4F AB 84 92 CF E0 FA 05 D3 DD EC
      :    F6 8C EB E8 0D 0A 96 1E 3D 43 E0 6D 10 38 F4 80
      :    74 4E 7A FA EF D9 3E A5 DF BE A8 9A 13 1F 1F 20
      :    1B B4 E9 A7 65 E9 3E 11 6C 2F 04 33 00 CC 92 8F
      :    49 34 83 31 F8 A2 19 34 F3 C0 31 70 1A C2 A3 81
      :    03 8D C8 6E 25 3C DE 8A C8 7F 16 9B A7 B9 CD D4
      :    7D 8D 8F F2 8D 33 1F 79 4C 3C 71 75 BE 1C C2 7E
      :    BF 9F 76 72 D9 99 C2 C5 6D 01 69 EF 4C 14 7A 54
      :    A8 89 6A 9C 8F 19 1F FA 03 15 A6 F2 6B 69 4C 04
      :    F5 6A 40 ED 11 02 2D DC 70 58 62 25 45 DA E9 68
      :    91 2F C4 8C 60 D3 7F 56 A2 40 D3 6D 2A 03 3D D2
      :    2A B8 15 49 7D AB A8 19 FF DB 98 78 37 98 54 CB
      :    F9 BA 7A F2 57 FF B7 D8 54 34 97 63 18 A4 01 9B
      :    7F E0 3C C5 ED E7 1C 14 BF 4E 8F CB A2 B2 24 0F
      :    8B CD 97 AD 80 A7 42 12 5E DF 2E C5 D6 61 86 83
      :    72 6B 02 C5 45 E7 69 C6 49 64 D7 B3 43 59 29 DC
      :    6E 91 8D 80 DD 11 2B A0 7B EF F9 08 AF B3 A3 97
      :    18 87 04 AA FB 08 6D 1C C9 AE FD 77 64 D4 CA 2D
      :    06 A9 D2 29 43 25 D0 E4 00 DD D7 3A 51 BA 6A 36
      :    9B A2 98 E3 72 BE 42 FB 8D 4A DD C6 35 95 05 BD
      :    3F E6 21 0A 70 20 19 E9 1F FC 19 40 A5 45 0A 2D
      :    CE F7 01 EF 58 7F D7 56 3D 79 87 98 56 E6 D7 5F
      :    88 63 9E 9F DE 6D D9 67 19 EF 28 66 11 84 AE 31
      :    A1 43 C1 24 C7 15 42 56 42 33 AE 4E 3E 43 F5 EC
      :    98 79 7E CD 20 71 04 74 17 8D 26 37 1C 5A DC DA
      :    A9 09 6D 44 C8 F6 BB B9 B4 3D 63 5B 33 66 7F 05
      :    55

```



```

864 3:    INTEGER 65537
      :    }
      :    }
      :    }
869 354: [3] {
873 350: SEQUENCE {
877 15:  SEQUENCE {
879 3:   OBJECT IDENTIFIER basicConstraints (2 5 29 19)
884 1:   BOOLEAN TRUE
887 5:   OCTET STRING, encapsulates {
889 3:   SEQUENCE {
891 1:   BOOLEAN TRUE
      :   }
      :   }
      :   }
894 88: SEQUENCE {
896 3:  OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
901 81: OCTET STRING, encapsulates {
903 79: SEQUENCE {
905 77: SEQUENCE {
907 4:  OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
913 69: SEQUENCE {
915 67: SEQUENCE {
917 8:  OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
927 55: IA5String
      : 'http://www.firma.infocert.it/documentazione/manu'
      : 'ali.php'
      : }
      : }
      : }
      : }
      : }
      : }
984 193: SEQUENCE {
987 3:  OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
992 185: OCTET STRING, encapsulates {
995 182: SEQUENCE {
998 179: SEQUENCE {
1001 176: [0] {
1004 173: [0] {
1007 38:  [6] 'http://crl.infocert.it/ca3/tsa/ARL.crl'
1047 130: [6]
      : 'ldap://ldap.infocert.it/cn%3DInfoCert%20Time%20S'
      : 'tamping%20Authority%203,ou%3DTSa,o%3DINFOCERT%20'
      : 'SPA,c%3DIT?authorityRevocationList'
      : }
      : }
      : }
      : }
      : }
1180 14: SEQUENCE {
1182 3:  OBJECT IDENTIFIER keyUsage (2 5 29 15)
1187 1:  BOOLEAN TRUE
1190 4:  OCTET STRING, encapsulates {
1192 2:  BIT STRING 1 unused bit
      : '1100000'B
      : }
      : }
1196 29: SEQUENCE {
1198 3:  OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1203 22: OCTET STRING, encapsulates {
1205 20: OCTET STRING
      : 2D 92 36 1F 33 B5 37 08 A8 4A 76 1C 1B 21 F1 77

```

```

:      C2 9F FA 44
:      }
:      }
:      }
:      }
:      }
1227 13: SEQUENCE {
1229 9:  OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1240 0:  NULL
:      }
1242 513: BIT STRING
:  BC 1B 66 5F 2F 0B AA 17 DA 1D 82 62 F9 64 C8 9D
:  61 01 48 06 27 F2 2E 38 64 67 11 7B D5 4B 87 4A
:  91 03 E9 FB 75 26 47 8D 18 9D D1 B5 BB 40 93 7B
:  23 56 C7 AF 21 CA 45 DF AD EB 01 86 86 AD 16 D8
:  63 7F DE 3E C4 83 29 3B 65 B3 35 1A 77 CA 7A B7
:  53 DB DF 9C EB DD A1 45 24 05 CB D7 BE BE DE 2B
:  E6 D1 9D 21 5F 10 D1 33 17 EB 1E DD 55 5D 21 25
:  0E 9D 6E 65 35 D6 AA A4 81 AF F5 57 FD E5 72 73
:  22 0F 28 03 FE 1E 89 90 56 13 61 FA 97 08 95 3D
:  DE EB CA 6A 22 6C 86 4B 9F 0E 30 D1 97 C8 37 12
:  AF 83 EC 2C 77 82 F0 48 F2 EC 77 61 63 0F 59 86
:  94 D9 00 48 59 3D E7 C2 3C 34 5E 4C 37 30 A2 54
:  9D D7 6D C7 35 6B ED F3 F2 43 BA 7B 9C 6C 75 32
:  F6 9C 7A 20 79 60 55 64 B3 92 AA 82 68 4D 02 BC
:  4B 60 A6 DB E6 B6 DB 06 2E 96 A2 4B BE 1B 89 0D
:  3B A1 5D 39 0C E0 24 52 2A C2 B9 E8 75 68 64 A5
:  3F 44 DB B8 4F D7 48 31 32 39 F2 4F B6 94 B6 21
:  B5 1F 78 C7 47 65 6E BF 85 54 E5 B0 82 15 92 36
:  1B 74 65 0C 8E 43 9B 4E 05 B1 C3 A7 CE 1B 8F 64
:  F4 1E 89 76 32 04 89 F7 17 02 1D A4 1A B2 9B 90
:  E2 29 EA D0 DA 72 A9 2C EB 87 AA 7C 12 B2 EA B6
:  8A 7F F2 39 0F 71 E2 62 EC FE 99 55 95 BF 61 F7
:  33 D3 BF F1 C3 5E 77 D0 EB 3D AC BE 73 22 7A 6B
:  1B B9 F8 FE 44 C0 3D 4F F0 E7 6E 97 89 74 F1 F4
:  56 58 8E 4B 05 A9 BE 6B D8 B5 35 64 A6 75 97 69
:  E3 C5 70 67 BE DD 5B 4B B6 6E F1 27 E9 E0 E2 06
:  D8 FE CF 7E 1D C5 54 3F CC 90 3C 04 79 22 F8 5D
:  CC 06 BC 3A 99 ED 95 44 9E C3 34 4F 31 8B DE 2F
:  E0 D9 66 3E 71 7E 82 72 82 0B E1 D7 D4 41 2D 04
:  AE 82 2D C8 85 6B 1B 8D 23 3D 4A 99 CD D5 07 A5
:  3C 98 B6 D2 08 22 9C 35 0A 34 03 4A 85 3F 89 3B
:  D2 38 A3 F3 E0 76 68 9F DA 23 0B 5F EE 1D C7 4C
:  }

```

Caution

Some formats allow you to enter the executable code (macros or commands) inside the document without this altering the binary structure and activating features that can modify the acts, facts, or data represented in the document itself. Digitally signed files containing such structures do not produce the effects referred to in Article 25 paragraph 2 of the Regulation [1], that is, it cannot be considered equivalent to an autograph signature. The owner must ensure, through the typical features of each product, the absence of such executable code.