Coloriuris Trust Services Provider

Policies and Practice Statements of the Time Stamping Authority

Author	Coloriuris S.L.
Version	1.0.1
Document status	Approved
Issuing date	01/03/2018
OID (Object Identifier)	1.3.6.1.4.1.37799.20.5.0.1.0
Document location	https://cipsc.coloriuris.net/politicas/

Index

Document Change History

History of the Document			
Version	Date	Description	Author
1.0	06/21/2017	Policies and practice statements of the Coloriuris Trusted Services Provider Time Stamping Authority	Coloriuris SL
1.0.1	07/04/2017	• Certificate profile correction • Update of the TSU Certificate data • Attached new anex with Policies revision	Coloriuris SL
1.1	01/03/2018	• Added new v3.1 CA and Issuer • Update translation	Coloriuris SL

1.- Basic declaration of the service

The Basic Statement of the CIPSC Time Stamping Service (TSACI) lists the key conditions and aspects of use of time stamping services which, along with other more specific conditions and aspects, are set out in this document. The content of this basic declaration corresponds to the TSA Disclosure Statement by the standard ETSI EN 319 421, whose functions this section fulfills to all effects.

This document is based on and expands the CIPSC Policies and Statement of General Practice statement with OID 1.3.6.1.4.1.37799.0.3.1.3.0, hereinafter DPPG.

Accordingly, by this basic statement, TSACI states that:

Ownership

The Coloriuris Time Stamp Authority (TSACI) is a service of Coloriuris S.L., company whose contact details are in section 1.6.4 of the "DPPG".

Availability of service

The TSACI certification service is available on an uninterrupted basis every day of the year, except for the on site processing of applications, which will only be available in the office hours established by each of the Registration Authorities.

Interruptions of services may be scheduled when strictly necessary for technical reasons, in which case they must be announced at least 24 hours in advance in the directory indicated in section 1.6.3 of the "DPPG".

Publication of the Policy

Each and every one of the time stamps issued by TSACI contains the identifier (OID) of this Policies and Practice Statement, which is included on the cover of this document.

Cryptographic mechanisms

The cryptographic algorithms and the length of the keys used in the issuance of the seals by TSACI comply with the ETSI standard EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles are as follows:

- The following algorithms are supported for the hash of the time stamp requests: SHA-256.
- SHA-256 is used to calculate the hash of the time stamps issued.
- The signature of the time stamps issued is done by calculating the hash using SHA-256 and encrypting it with RSA algorithms, using a key with a length of at least 2048 bits.

Validity of time stamps

TSACI does not establish other limitations on the reliability of its time-stamping services than those inherent in the technologies used. If it is determined that the cryptographic algorithms or the length of keys used have failed to provide an adequate level of security, TSACI will immediately publish such information on its website.

Temporary Accuracy

TSACI ensures that the time fixed on the stamps is within the margin of error established in section 2.3 of this document, in relation to the time established by the trusted UTC time sources defined in section 3.4 and guarantees that it will not issue stamps of Time with less precision than the above.

Applicability

TSACI considers that the most appropriate uses of the time stamps issued are those related to proof of the occurrence of events that have or may have legal effects, such as those described in section 2.5 of this document. Seals issued by TSACI cannot be used in applications where time-dependent controls require automated actions that, in the event of failure or error, may result in material or personal injury.

Obligations

The obligations of the user parties are described in sections 2.6 of this document and in section 2.3.3.

Registration of operations

TSACI registers its operations and keeps this information in adequate security conditions, as provided in sections 3.3.4 of the "DPPG".

Normative

The provision of the time stamp service by TSACI is carried out in accordance with the Spanish and European legislation applicable to the subject, with the present Policies and declaration of practices and with the internal regulations of Coloriuris.

Responsibility

The responsibilities of TSACI and the limitations established therein are described in section 2.4 of the "DPPG".

Complaints

All claims by users and third parties regarding the provision of time-stamping services by TSACI shall be communicated as established in section 2.8.1 of the "DPPG". In the event of failure to reach an agreement between the parties, these will be submitted to the courts and tribunals specified in section 2.8.2 of the "DPPG", expressly renouncing any other jurisdiction that may correspond to them.

Warranty and audits

TSACI guarantees that the provision of time-stamping services is in accordance with what is established in these Policies and declaration of practices. According to the same Coloriuris conducts periodic audits of the operation of the Time Stamping Authority.

Rates

TSACI may request an economic consideration for the issuance of its time stamps, in accordance with the fees that are published at any time on its website.

2.- Policy for the delivery of the service

2.1.- Introduction

This Policy regulates the generation and issuance of time stamps by TSACI in accordance with the technical specification ETSI EN 319 421. The private key used and the time-stamping unit (TSU) comply with the technical specifications of the standards: ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

TSACI uses a specific private key for the signature of the time stamps. Each seal issued contains the identification of the Policies and declaration of practices that apply to it.

2.2.- Versions

This version of the TSACI Policy and Practice Statement replaces all effects and from the time of its publication to the Time Stamp Seal Policies and Practices of the Coloriuris Time Stamping Authority SL, dated 10-13-2015 And with OID: 1.3.6.1.4.1.37799.0.3.1.2.0.

2.3.- Precision

Time stamps (TST) are issued with an accuracy ± 1 second UTC.

2.4.- User community

The community for the generation, issuance and use of these certificates are the Time Stamping Authority (TSACI), as described in the "DPPG" in sections 2.1.2.1 and 2.1.2.3 and the user parties, as described in Section 2.2.2 of said "DPPG".

TSACI is responsible for the issuance and management of time stamps. The user parties are those who rely on the time stamps issued by TSACI.

All of them will be subject to the provisions of this Policy.

2.5.- Uses of time stamps

The time stamps issued in accordance with this policy are designed to prove the timing of events and acts, with the main purpose of being used in legal contexts. For example, the following are typical uses of the TSACI seals:

- Provide temporary certainty to electronic signatures
- Preserving electronic signatures in files of long term validity
- To prove that certain data existed before a given moment

- To accredit the moment in which an act and / or legal process is carried out, including the certified electronic delivery.
- And, in general, its use in archives of electronic documents, databases, registration systems and logs.

TSACI time stamps cannot be used in critical applications where a service failure or error could involve any kind of material or personal injury.

2.6.- Obligations

In addition to the obligations established by law and those listed in section 2.3 of this document, the following specific obligations are established for the provision of time-stamping services.

TSACI

1) Keep the clock of the TSU synchronized with the declared accuracy with respect to UTC time.
2) Provide uninterrupted access to time-stamping services except in case of scheduled outages, loss of temporary synchronization or serious incidents.

User Parties

1) Use appropriate means to request and obtain time stamps.
2) Use time stamps only for uses and for the purposes permitted in this Policy.
3) Check the validity of the time stamps.
4) Do not rely on time stamps for uses other than those permitted in this Policy.
5) Report any incidents or anomalous situation related to the sealing service, and / or time stamps issued, and that can be considered as cause of revocation of the same.

2.7.- Registration of information regarding the operation of time-stamping services

TSACI maintains records of all relevant information regarding its operations, as established in sections 3.3.4 of the "DPPG". In addition to those provided in this section, the CA keeps records of the following events:

- Petitions for the emission of time stamp
- Emission of time stamps

3.- Declaration of practice

3.1.- Access to the service

Users can request time stamps as provided in the TSP Time-Stamp Protocol (RFC 3161) protocols.

The access address to the service is: https://cipsc.coloriuris.net/tsa/

3.2.- Availability of the service

TSACI's time-stamping service is available uninterrupted.

Interruptions of services may be scheduled when strictly necessary for technical reasons, in which case they must be announced at least 24 hours in advance in the directory indicated in section 1.6.3 of the "DPPG".

When the interruption is due to force majeure or serious incidents, CIPSC will act with the utmost diligence to get the services started, as well as to minimize the possible damages that have been caused to the signatories, sealers and / Or user parties.

3.3.- Life cycle of keys

The generation and protection of the private keys in use by TSACI TSUs is carried out following the recommendations of ETSI EN 319 421 in sections 7.6.2 and 7.6.3 in cryptographic modules with the ratings indicated in section 3.4 .2.1 of this declaration.

The public keys associated with the private keys and their respective certificates will be available in the repositories indicated in the section 1.6.3 of the "DPPG".

3.4.- Time Stamp

TSACI adopts the necessary technical measures to ensure that its time stamps are safe and include the correct date and time. Seals are issued using a cryptographic device (TSU).

The time stamps generated conform to the standards referenced in the annex to this document, and their format and content is specified in RFC 3161 Time-stamp Protocol (TSP). All seals include at least the following content:

- The identifier of the applicable Policy, whose value is indicated in section 1.5.
- The hash of the dataset whose existence at that moment is believed.
- A unique serial number that identifies the time stamp.
- The time, expressed in the Universal Coordinated Time (Zulu Time) format.
- The electronic signature of the seal, generated by the TSU.

As an attachment to the seal, users are given the electronic certificate that supports the signature incorporated into the seal. Section 3.6 describes the certificates used by CIPSC for this purpose, which fully identify the TSU and CIPSC.

TSACI audits the accuracy of the time source and will not issue time stamps if its accuracy is outside the established range.

3.5.- Clock synchronization with UTC

TSACI provides the time instant with the accuracy stated in section 2.3 of the Policy, taking as a reference a safe source of time from among the following:

- Time source stratum 1 through the NTP protocol. This time source provides precision at the microsecond level using synchronization with the Navstar satellite system.

- Royal Institute and Observatory of the Navy (ROA), which according to the provisions of the R.D. 1308/1992, dated October 23, is responsible for the maintenance and official dissemination of the "Universal Coordinated Time" (UTC-ROA) scale, which is the basis of the legal time in the entire national territory. This signal is received through the NTP protocol via the Internet.

- From the atomic clock in Braunschweig, Germany, (Physikalisch Technische Bundesanstalt), which represents the official time within the Eurosystem. It is coded and transmitted by radio.

The clock used by the TSU is recalibrated periodically and automatically from the safe time source. It is also capable of detecting deviations from the established accuracy and activating a new calibration if necessary.

The clock and TSU are permanently located in a secure physical environment and are protected from unauthorized access, both physical and remote.

The events related to the synchronization and modification of the clock time relative to the safe time source are recorded in order to detect the deviations produced, either accidentally or intentionally.

3.6.- TSACI Root Certificate and Seals

3.6.1.- Root Certificates

The origin of the v3.0 TSACI trust chain is a self-signed certificate issued by CIPSC, with a key length of 4096 bits and a validity period of 20 years.

Its content is as follows:

Issuer	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Subject	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Public key	RSA (4096 Bits)
AIA Access Issuer Information	access id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt access id-ad-ocsp https://ocsp.coloriuris.net
Distribution point CRL	https://cipsc.coloriuris.net/crl/tsa/tsa-v3.crl
Certificate bases	[1] Certificates Directive: Directive identification=2.5.29.32.0 [1,1]Policy certifier information: Policy certifier identifier=CPS Certifier: https://cipsc.coloriuris.net/politicas/
Key usage	Certificate signing, offline CRL signing, Certificate Revocation List (CRL) signing
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements

QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)

The origin of the v3.1 TSACI trust chain is a self-signed certificate issued by CIPSC, with a key length of 4096 bits and a validity period of 20 years.

Its content is as follows:

Issuer	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3.1
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Subject	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3.1
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Public key	RSA (4096 Bits)
AIA Access Issuer Information	access id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt access id-ad-ocsp https://ocspv3.coloriuris.net
Distribution point CRL	https://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl
Certificate bases	[1] Certificates Directive: Directive identification=2.5.29.32.0 [1,1]Policy certifier information: Policy certifier identifier=CPS Certifier:

	https://cipsc.coloriuris.net/politicas/
Key usage	Certificate signing, offline CRL signing, Certificate Revocation List (CRL) signing
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)

3.6.2.- Certificates for the issuance of time stamps

TSACI will have two qualified certificates for the issuance of time stamps, issued by CIPSC's own TSACI using its root certificate, and whose period of validity will be 10 years.

The profile of this certificates will be based on 2048 keys for the issuance of time stamps and identified by OID 1.3.6.1.4.1.37799.20.5.1

V3.0 certificate profile:

Issuer	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Subject	
CN	CIPSC - v3 – Emisor de sellos de tiempo de 2048
OU	Emisión de sellos de tiempo
organizationIdentifier (2.5.4.97)	VATES-B99091696
O	Coloriuris S.L.
L	Zaragoza
C	ES
Public Key	RSA (2048 Bits)

AIA Access Issuer Infomration	access id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt access id-ad-ocsp https://ocsp.coloriuris.net
CRL Distribution point	http://cipsc.coloriuris.net/crl/tsa/tsa-v3.crl
Certificate basis	[1]Certificates Directive Directive identification=1.3.6.1.4.1.37799.20.5.1 [1,1]Policy certifier information: Policy certifier identifier=User Notice Text Certifier: Notice Text=Certificado cualificado de emisión de sellos de tiempo electrónicos [1,2]Policy certifier information: Policy certifier identifier=CPS Certifier: https://cipsc.coloriuris.net/politicas/
Uso de la clave	Digital signature, Non repudiation
Uso extendido de la clave	Time Stamping
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)
EuQCompliance	Id-etsi-tsts-EuQCompliance (0.4.0.19422.1.1)
Key usage	Timestamping, No repudiation

V3.1 certificate profile:

Issuer	
E	cipsc@coloriuris.net
CN	CIPSC - Raíz de la Autoridad de Sellado de Tiempo v3.1
organizationIdentifier (2.5.4.97)	VATES-B99091696
OU	Prestador de servicios de Confianza
O	Coloriuris S.L.
L	Zaragoza
C	ES
Subject	
CN	CIPSC – v3.1 – Emisor de sellos de tiempo de 2048

OU	Emisión de sellos de tiempo
organizationIdentifier (2.5.4.97)	VATES-B99091696
O	Coloriuris S.L.
L	Zaragoza
C	ES
Public Key	RSA (2048 Bits)
AIA Access Issuer Infomration	access id-ad-http https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt access id-ad-ocsp https://ocspv3.coloriuris.net
CRL Distribution point	http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl
Certificate basis	[1]Certificates Directive Directive identification=1.3.6.1.4.1.37799.20.5.1 [1,1]Policy certifier information: Policy certifier identifier=User Notice Text Certifier: Notice Text=Certificado cualificado de emisión de sellos de tiempo electrónicos [1,2]Policy certifier information: Policy certifier identifier=CPS Certifier: https://cipsc.coloriuris.net/politicas/
Uso de la clave	Digital signature, Non repudiation
Uso extendido de la clave	Time Stamping
1.3.6.1.5.5.7.1.3 -IETF / 0.4.0.1862.1.1-ETSI	Qualified Certificate Statements
QCSyntax-v2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)
EuQCompliance	Id-etsi-tsts-EuQCompliance (0.4.0.19422.1.1)
Key usage	Timestamping, No repudiation

Annex I

Acronyms used

- **CA:** CIPSC Authority for the provision of trusted services
- **RA**: Registration Authority
- **ASD**: CIPSC authority for the provision of services relating to electronic documents
- **CEN-CWA**: European Committee for Standardization - CEN Workshop Agreement
- **CIPSC**: Coloriuris Trusted Services Provider
- **CN**: Common Name. Distinctive Name (DN) attribute of an object within the X.500 directory structure
- **CRL**: Certificate Revocation List
- **DSCF**: Secure Signature Device
- **EAL**: Evaluation Assurance Level
- **ETSI**: European Telecommunications Standard Institute
- **FIPS**: Federal Information Processing Standard
- **HSM**: Hardware Security Module. Cryptographic security module used to store keys and perform cryptographic operations in a secure way.
- **IETF**: Internet Engineering Task Force (Internet Standardization Organization)
- **OASIS**: Organization for the Advancement of Structured Information Standard
- **OCSP**: Online Certificate Status Protocol. This protocol allows online verification of the validity of an electronic certificate.
- **OID**: Object identifier
- **PKI**: Public Key Infrastructure
- **PSC**: Trusted Services Provider
- **RFC**: Request For Comments (Standard issued by the IETF)

- **SSCD**: Secure Signature Creation Device
- **TSA**: Time-stamping Authority
- **TSACI**: CIPSC authority for the provision of the time-stamping service
- **TST**: Time-stamping Token
- **TSU**: Time-stamping Unit
- **UTC**: Coordinated Universal Time
- **XAdES**: XML Advanced Electronic Signatures

Definitions

- **CIPSC service authorities**: the authorities that provide each of the services of trust of CIPSC
- **Electronic signature certificate**: an electronic declaration linking the validation data of a signature with a natural or legal person and confirming at least the name or pseudonym of that person;
- **Electronic seal certificate**: an electronic declaration that links the validation data of a seal with a legal person and confirms the name of that person.
- **Session key**: a key that is generated specifically for a communication or session, ending its utility once it is completed.
- **Public key and private key**: asymmetric cryptography uses a key pair in which what is encrypted with one of them can only be decrypted with the other and vice versa, one of these keys is called public (it matches the data of Creation of the electronic signature) and is included in the electronic certificate, while the other is called private and is only known by the certificate holder.
- **Identification data of the person**: a set of data that allows establishing the identity of a natural or legal person, or of a natural person that represents a legal person;
- **Validation data**: the data used to validate an electronic signature or an electronic seal.
- **Statement of practice**: statement of practices that an Authority employs for the provision of its services.
- **Electronic document**: all content stored in electronic format, in particular, text or sound, visual or audiovisual record.

- **Evidence**: These are the authentic elements issued by CIPSC. They include, in particular, electronic certificates, time stamps and certificates of issue and receipt of certified electronic mail and, in general, any authentic electronic document issued as a result of the provision of a reliable service of CIPSC and expressly contemplated in These policies and practice statement.
- **Electronic identification**: the process of using the identification data of a person in electronic format that uniquely represent a natural or legal person or a natural person representing a legal person;
- **Time stamping policy**: set of rules that establish the applicability of the time stamp and its emission characteristics.
- **Certification service provider**: natural or legal person who issues electronic certificates or provides other services in connection with electronic signatures.
- **Trusted service provider**: a natural or legal person providing one or more trusted services, either as a qualified provider or as an unqualified provider of trust services.
- **Electronic time seal**: data in electronic format that links other data in electronic format with a specific time, providing evidence that the latter data existed at that time.
- **Time stamp**: a data structure that links certain data to a particular time instant, providing evidence of its existence before that moment.
- **Electronic stamp**: data in electronic format attached to other data in electronic format, or logically associated with them, to guarantee the origin and integrity of the latter.
- **Trusted service**: the electronic service usually provided for a remuneration, consistent in the creation, verification and validation of electronic signatures, electronic stamps or electronic time stamps, certified electronic delivery services and certificates relating to these services, or the creation, verification and validation of certificates for website authentication, or preservation of electronic signatures, seals or certificates relating to these services.
- **Certified electronic delivery service**: a service that allows the transmission of data between third parties by electronic means and provides evidence related to the management of transmitted data, including proof of shipment and reception of data, and which protects The data transmitted against the risks of loss, theft, deterioration or unauthorized alteration.
- **Signer**: individual who creates an electronic signature.
- **Creator of seal**: legal person that creates an electronic seal.

- **Part user**: natural or legal person who relies on Electronic identification or trusted service.
- **Coordinated universal time (UTC)**: time scale, based on the second, as defined by the International Telecommunication Union (ITU-T) Radio Committee TF.460-5.
- **Time-Stamp Unit (TSU)**: A set of hardware and software that is managed as a unit and which has a single active signature key at all times.
- **Validation**: the process of verifying and confirming the validity of an electronic signature or seal.

Regulations

The basic legislation applicable is the following:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, relating to the electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Law 59/2003, of 19 December, on Electronic Signature.
- Organic Law 15/1999 of 13 December on the protection of personal data
- Royal Decree 1720/2007, of 21 December, approving the Development Regulation of Law 15/1999 of 13 December on the protection of personal data
- Law 34/2002, of 11 July of Information Society Services and Electronic Commerce.
- Technical Standard for Interoperability (NTI) Electronic Document (Resolution of the Secretary of State for Public Service, of 19 July 2011)
- NTI of reuse of information resources (Resolution of 19 February 2013)
- NTI policy of management of electronic documents (Resolution of 28 June 2012)

Standards

The content of the following documents is relevant for the development and / or application of these Policies and practices declaration of Coloriuris Trusted Services Provider:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates V1
- A/Browser Forum EV SSL Certificate Guidelines V 1.3

- ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures.
- ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy requirements for Trust Service Providers issuing qualified certificates; Part 1: General requirements.
- ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy requirements for Trust Service Providers issuing qualified certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 122, Electronic Signatures and Infrastructures (ESI); CAdES digital signatures;
- ETSI EN 319 132, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures;
- ETSI EN 319 412, Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
- ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ISO/IEC 18014-1, Time-stamping services — Part 1: Framework
- RCF 3647, *Internet X.509 Public Key Infrastructure Certificate Policy*
- RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
- RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 3739 y 3039, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*
- RFC 5280 y 3280, Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)

Signed.: Pedro Canut Zazurca
Head of Policy Management at Coloriuris S.L.
Date: 01/03/2017

Annex II - TSACI Certificates

[TSA] V3.0 Root Certificate

Subject	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza organizationIdentifier = VATES-B99091696 CN = CIPSC - Raíz - Autoridad de Sellado de Tiempo v3 E = cipsc@coloriuris.net
Validity	De 06/21/2017 a 06/21/2037
Hash (SHA1)	01 C4 76 53 40 6D 53 F3 61 51 01 06 51 40 3C 47 BB 46 37 8B
Download URLs	DER https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt PEM https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.pem

[TSA] V3.0 Qualified Certificate for TimeStamping

Subject	C = ES L = Zaragoza O = Coloriuris S.L. organizationIdentifier= VATES-B99091696 CN = CIPSC – v3 - Emisor de sellos de tiempo de 2048
Validity	De 07/04/2017 a 07/04/2027
Hash (SHA1)	B5 F9 09 C0 21 F2 F6 2B B4 72 23 9D 84 5C B6 4E 06 B9 B1 01
Hash (SHA256)	D89C1C4E9477B4768B1C46F7E16129541CCDE19951A4912AF65743E7BD5513BE
Download URL	https://cipsc.coloriuris.net/certificados/tsa-v3/tsu/2048.crt

[TSA] V3.0 Root Certificate

Subject	C = ES L = Zaragoza O = Coloriuris S.L. OU = Prestador de Servicios de Confianza

	organizationIdentifier = VATES-B99091696 CN = CIPSC - Raíz - Autoridad de Sellado de Tiempo v3.1 E = cipsc@coloriuris.net
Validity	De 21/12/2017 a 21/12/2037
Hash (SHA1)	F9 F0 87 AC F2 65 2C D0 CF E1 0C 98 18 AC A9 91 3D BC 8F 28
Download URL	DER https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt PEM https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.pem

[TSA] V3.1 Qualified Certificate for TimeStamping

Subject	C = ES L = Zaragoza O = Coloriuris S.L. organizationIdentifier= VATES-B99091696 CN = CIPSC – v3.1 - Emisor de sellos de tiempo de 2048
Validity	De 01/07/2017 a 01/07/2027
Hash (SHA1)	93 DF B8 89 2B 2D AA 5B 51 0E C4 9C 1B 0A B8 7B 59 7C 13 60
Hash (SHA256)	8589DC8BADF04DF2FB0F9063026950D1894941903C845CD9B15C5BC18FAE6DC3
Download URL	https://cipsc.coloriuris.net/certificados/tsa-v3.1/tsu/2048.crt

Annex III

Descriptive table with the identifying OIDs of the final certificates in use by the TSACI services.

OID Base assigned by IANA for Coloriuris: **1.3.6.1.4.1.37799**

1.3.6.1.4.1.37799	.20	End Certificate Profiles for CIPSC services		
		.5	Time Stamping Authority	
			.1	Qualified Certificate for Time Stamping

Annex IV – Policy Review

These policies will be reviewed every 6 months (regular review) and whenever there is any legislative change and / or in the applicable ETSI standards. Policies will also be reviewed each time a new trusted service is activated or there is a cessation of any of the trusted services provided by CIPSC.

The policy review will be carried out by the policy manager, who will review the official pages of the Ministry of Energy, Tourism and Digital Agenda, ETSI and the European Union (or bodies that could replace them in the future) With semiannual cadence in order to check if there have been changes that need a modification of them.

In the event that there are no changes that apply to the policies of Coloriuris, an act will be drawn up which will be transferred to the Directorate for approval.

In the event that if there are changes that apply to the policies of Coloriuris, an act will also be drawn up, which will be sent to the Directorate for approval. Likewise, the new version of the policies, with the changes in the document, will be communicated to the national regulator requesting the latter to decide on the need to submit the changes to the conformity assessment body.

The changes produced will be published in the CIPSC electronic site both in the url of these policies and in the section / announcements.

Likewise, notifications of legislative changes and / or ETSI rules that apply to the present policies by the Regulator and / or user parties will be carried out.

The necessary policy changes will be carried out immediately.