Coloriuris Trust Services Provider

General Policies and Practices Statement

Author	Coloriuris S.L.
Version	3.1
State of the document	Approved
Date of issue	04/09/2018
OID (Object Identifier)	1.3.6.1.4.1.37799.0.3.1.3.1
Location of the document	https://cipsc.coloriuris.net/politicas/

Contents

Document History

History			
Version	Date	Description	Author
3.0	06/21/2017	• First version translated to english	Coloriuris SL
3.0.1	07/02/2017	• Added annex with policy revision	Coloriuris SL
3.0.2	01/03/2018	• Translation revision • Update of the CRL issuing period	Coloriuris SL
3.1	04/09/2018	• Retire explicit references to services other than timestamping	Coloriuris SL

1. The policies and practices of Coloriuris Provider of Trust Services

1.1.- Purpose

Coloriuris S. L. is a company specialized in providing security services for the execution of legal acts on the Internet and the use of electronic documents. To this purpose, the company is established as a trusted service provider under the name of "Coloriuris Trusted Service Provider (hereinafter CIPSC)" in accordance with Law 59/2003 of December 19, of Electronic signature and in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trustworthy services for electronic transactions in the internal market and repealing Regulation Directive 1999/93 / EC.

The activity of CIPSC is governed by whatit is established in this document that complies, insofar as it relates to the purpose and contents, with the established by the following norms:

- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*
- ETSI EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.*
- ETSI EN 319 422 *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.*

The provisions set forth herein apply to all parties involved in CIPSC services, including signatories, creators of electronic stamps and user parties. All of them must know the content of this document so that they can establish their trust in the services provided by CIPSC and adapt their performance to the provisions thereof.

This document may also be used by third entities and independent bodies to verify and certify that CIPSC acts in accordance with the policies and practices contained therein.

1.2.- Structure

CIPSC provides the following services:

- Creation, verification and validation of electronic time stamps

This document governs in the first place the aspects common to all these services, in the following chapters:

Legal Regime

It sets out the rights and obligations of the different parties involved in the provision of services of CIPSC confidence, as well as the legal framework in which these are developed and the mechanisms for the resolution of conflicts.

Policy for the provision of trust services

Aims to define the requirements to be met by CIPSC for the provision of trust services, in accordance with the standards that are applicable. Defines the aspects that are common to the whole of the services.

Statement of Practice

Sets how CIPSC meets the technical requirements, organizational and procedural aspects common to the various services and that have been established in the policy for the provision of trust services.

Then, for each of the services include the following sections:

Basic Statement

The basic statement reflects the conditions and fundamental aspects of the service, which, together with other conditions and more specific aspects, are reflected in the relevant policy.

Policy for the provision of the service

Aims to define the requirements to be met by CIPSC for the provision of a service of trust, in accordance with the standards that are applicable. Are defined aspects as the assumptions of use, the recipients, the conditions for the provision and access to the service and the effects of the same.

Statement of practices for the provision of the service

Sets how CIPSC meets the technical requirements, organizational and procedural requirements set out in the Policy of the service, and in particular, the conditions and the actions of management and operation that are followed in the delivery of the same.

1.3.- Scope

This document sets out the general rules for the operation of CIPSC and the provision of particular services, the CIPSC obligations in connection with the management of the data creation and signature verification and of electronic certificates, the conditions applicable to the request, issuance, use, suspension and termination of the validity of the certificates, the technical and organizational security measures, the profiles of the certificates and the mechanisms of information on the observance of the certificates.

1.4.- Scope of application

The CIPSC services are provided subject to the version of this document, which is in effect at the time are effective, that will determine its validity and effects. When the service consists in the generation and/or issuance of electronic signatures, electronic stamps, time stamps, electronic certifications of referral and receipt of electronic submissions, of authentic documents and proceedings of registration or any other electronic evidence will be these policies that will establish the validity and effect of the same throughout its life cycle.

1.5.- Identification

The OID (*Object Identifier*) of the policies and practices of Coloriuris Provider of Trust Services is: 1.3.6.1.4.1.37799.0.3.1.3.1.

1.6.- Administration and advertising

1.6.1. Validity

Only the Head of Administration Policy has the ability to approve the policies and practices of CIPSC. This approval shall be expressly stated.

Without prejudice to the provisions for the modification of policies and practices, and in the event of termination of activity of CIPSC, the purpose of this document is valid indefinitely.

The invalidity of one or more of the provisions of these policies and practices statement shall not affect the remainder of the document. In this case these forecasts will not aplly.

1.6.2. Modifications

Only the Head of Administration Policy can perform and approve modifications of policies and practices statement of CIPSC.

It is considered that there is a version change when, in the opinion of the officer Responsible for Administration Policy changes may affect the acceptability of the CIPSC services. Otherwise it is considered that there is only one new wording of the same version.

In the first case will proceed to the increase of the major version number of the document and the zeroing of the minor number of the same, and also the corresponding fields in the object identifier (OID), which are the penultimate and the last, respectively. In the second course will increase in the minor version number of the document, changing only the last field in the Object Identifier (OID).

1.6.3. Notices

The policies and practices of CIPSC will be issued immediately from the time of its initial approval and, where appropriate, of its modification. The web address (URL) for the publication will be:

https://cipsc.coloriuris.net/politicas/

It will also be posted on the web root certificates and stamps of the authorities supplying services of CIPSC. This publication will be made at the following address:

https://cipsc.coloriuris.net/certificados/

The postal address of CIPSC is posted at:

https://cipsc.coloriuris.net/address/

The publication of notices and information about relevant events that affect the provision of the services of the CIPSC, shall be made in the Internet address:

https://cipsc.coloriuris.net/anuncios/

Finally, the publication of the rates applicable to the provision of particular services of CIPSC will be published in the address:

https://cipsc.coloriuris.net/tarifas/

These contents are permanently available, except in cases of force major, and the access to the same will be free.

1.6.4. Contact Information

All signatories, creators of stamps , third acceptors and any entity or person having a legitimate interest in connection with the services of CIPSC may be put in contact with members of the same in the following ways:

E-mail: cipsc@coloriuris.net
Phone: +34976203670
Fax: +34976203671
Postal Mail or being represented at the address: C/ Alfonso I nº 23, entlo. ctro., 50003 Zaragoza

2. Policies of the CIPSC services

2.1.- Structure of CIPSC

2.1.1. Responsible for administration of policies of Coloriuris

The officer Responsible for Administration of policies is a member of Coloriuris to approve the present policies and practices, as well as its amendments. All policy documents and CIPSC practices statement must be approved by the officer responsible for Administration of policies.

The Responsible Policy Management is responsible for the provision of the services of the CIPSC conforming to the provisions in these policies and practices and to ensure the effective implementation of the controls provided for. It also is responsible for the direction, supervision and control of the provision of the services of CIPSC, of the operative followed by each of its service providers and authorities of the correct implementation by the same as set forth in this document.

The Responsible Policy Management is also responsible for analysing the reports of the audits, full or partial, made of CIPSC and of its services, as well as to establish and monitor, in his case, the corrective actions to be executed.

The officer Responsible for Administration of policies shall be appointed and removed by the direction of Coloriuris, by means of explicit resolution of which shall be written record.

2.1.2. Authorities providing trust services of CIPSC

2.1.2.1. Common Aspects

CIPSC has one authoritie providing services, which is attached to the policies and practices set forth in this document and it is the following:

- Time Stamping Authority (TSACI): responsible for the generation and issuance of time stamps.

Each authority can have one or more self-signed certificates, and can also have certificates backed by those root certificates, which shall be issued by the authority's own service provider. The keys associated with these certificates are kept in a cryptographic device with security levels set forth in these Policies.

In any case, CIPSC will be identified in the electronic certificates root of each one of its competent service providers, as well as certificates issued for each of the services, both in the case of electronic stamps as personal certificates of administrators and operators, and the evidences that are a result of the provision of one of their services.

Administrators of each of the authorities are the people inside of Coloriuris have privileges to generate and use the certificate and root keys of that authority, as well as the stamps derived from it. At any time these people will be explicitly identified in the internal documentation of the CIPSC.

2.1.2.2. Time Stamping Authority (TSACI)

The services it provides are the following:

- Creation, verification and validation of time stamps: includes the technical and organizational components that emit the time stamps.
- Management of the service of time: includes the technical and organizational components that monitor and control the operation of the emission of time stamps to be carried out in an appropriate manner including, in particular, the synchronization with the reliable source of reference.

2.1.3. Registration Authorities

Registration Authorities (AR) Receive and process applications for the provision of trust services by CIPSC and fulfill the other functions which, in its case, are laid down in the relevant policies. In any case, perform the following tasks:

- Reception of the data required for the provision of the services and, in its case, checking the identity of the applicants, signatories and creators of stamps of the same as well as the other circumstances that may be required to provide the service.

- Reception and conservation of paper documents generated in the process of application and service delivery.

CIPSC shall include at least one AR included in its own structure. Optionally, you may create other AR CIPSC, both within and through external entities, in which case it will be necessary that there should be a written contract, in which the external entity must undertake to comply with the provisions of this document. It also established the obligation to perform audits, as well as the periodicity of the same. Audits may be carried out by Coloriuris or by an external entity.

The operators of the AR will have certificates issued by the certification authority of CIPSC sign electronically with the requests for the provision of services to the various authorities, when so set the corresponding policy. The telematic communication between AR and the various authorities will be made through encrypted channels.

2.2. Signers and parties users

2.2.1. Users

User parties are natural or legal persons who rely on electronic identification and trust services of CIPSC evidence and CIPSC generated as a result of the same, especially electronic signatures, electronic stamps, time stamps, electronic documents authenticated, certifications of referral and receipt of electronic delivery certified and registration proceedings.

2.2.2. Acceptance of the policies and practices statement

All signatories and creators of stamps of CIPSC services, by the mere fact of using them, as well as user parties, assume in full the provisions of the version of the Policies and practices in force at the time you received the service requested or accepted the evidence resulting from the same, respectively.

The OID of these policies and practices will be included in all the evidence that will be generated and issued on the provision of the services of the CIPSC as accreditation of their conformity with the same. To the same end, CIPSC will only accept requests for services that include the OID of these policies and practices statement or that, as a minimum requirement, do not include the reference to one or more other policies in such a way that it could be inferred from the accordance with the same.

2.2.4. Verification of the evidence

The signatories, creators of stamps and parts users must act with due diligence to verify the authenticity of the evidence from the CIPSC services, verifying that they have been signed correctly and that the private key used for signing was not committed at the time of verification. During the period of validity of the certificates used by the authorities providing the CIPSC services, the state of the private keys may be checked at the addresses indicated in paragraph 1.6.3.

Once they expire the certificates used by CIPSC user parties will be able to rely on the signatures supported by the same if at the time of verification, it is known that the corresponding private key has not been compromised at any time and that both the hash function used for the generation of evidence, as well as the cryptographic algorithm and the size of the key used to sign it electronically are still considered safe.

2.3.- Obligations

2.3.1. Coloriuris

Coloriuris assumes responsibility for ensuring that the services provided by CIPSC are carried out in accordance with the provisions of these policies and practices, and the compliance of the requirements and controls established in the same, as the legal provisions that are applicable. In particular, assume the following obligations:

1) To provide the services in accordance with the provisions of these policies and practices.
2) Ensure that the evidence issued do not contain any erroneous or false.
3) Use appropriate technologies and equipment, and staff with specific training and informed of their obligations.
4) Provide uninterrupted access to its services, except in the event of serious incidents or scheduled outages.
5) To carry out the reviews and audits to ensure compliance with applicable legislation, policies and practices and of the internal regulations.
6) Publish on its website information on the events that they have been able to affect the services in such a way that it is possible to know which have been, in his case, the evidence affected.

2.3.2. Obligations of the users

It is the obligation of the parties to the users to accept and trust the evidence issued by CIPSC:

1) To verify the validity of the evidence, according to the provisions of paragraph 2.2.4.
2) Do not rely on the evidence for uses other than those allowed in the policy.
3) Have knowledge of the provisions in these policies, accepting and subject to the provisions of the same and, in particular, to the responsibilities applicable in the acceptance and use of the services of the CIPSC and the evidence resulting from the same.
4) Notify any fact or anomalous situation relating to the service of the CIPSC and/or to the evidence given, and that can be considered as a cause for revocation.

2.4.- Responsibility of CIPSC

CIPSC shall only be liable in the event of non-compliance with the obligations contained in the applicable legislation and in the present policies and practices.

CIPSC does not assume any liability with regard to the use of evidence issued for any unauthorized use in these policies and practices.

CIPSC is not responsible for the content of documents and data to which they apply their services, and is not liable for any damages incurred in transactions that have been used.

CIPSC does not represent in any way the signatories, creators of stamps or parts, users of the evidence that it emits.

CIPSC does not give any warranty or assume any responsibility, to holders of certificates or any other evidence issued or to the parties to the users of the same, outside of what is established in the present policies and practices.

CIPSC has liability insurance with a coverage of three million euros (3,000,000.00 €).

2.5.- personal data and confidentiality

2.5.1. Protection of personal data

CIPSC applies the provisions of Law 15/1999 of 13 December on the Protection of Personal Data (LOPD) and its implementing regulations, ensuring the internal rules and procedures of Coloriuris to the implementation of the level of security required by these regulations.

When for the provision of a service is necessary to collect personal data, we will verify that this is informed and consent to the processing of their personal data, the purpose of this, and their inclusion in the file declared by Coloriuris.

The personal data will not be communicated to third parties without the express written consent of the holder, except in the case of a law that explicitly authorized.

2.5.2. Confidential Information

Shall be treated as confidential all information that is not expressly declared by CIPSC as public. In particular, is of a confidential nature the following information:

- The private keys used by CIPSC and by their managers and operators.
- The information on the operations of CIPSC.
- Safety information, control and audit procedures.
- The personal information of the signatories.

It is considered public information and therefore accessible by third parties contained in these policies and practices, and another that is declared by CIPSC.

2.5.3. Duty of secrecy

All persons who have professional or employment relationship with CIPSC are required to maintain the secrecy of all confidential information to which they have access by virtue of that relationship. CIPSC inform them in writing, at least in the beginning of the relationship, fixing on record that that information has been received by the addressee. This obligation will persist once the purpose of linking with CIPSC.

2.6.- Audits

Coloriuris will conduct audits of the operation of the CIPSC and the authorities in charge of providing different services, at least on an annual basis. Audits should be carried out by an independent auditor. In addition, as provided for in paragraph 2.1.3, audits will be carried out to Registration Authorities, both at the integrated into the structure of the external CIPSC. These audits will be carried out at least every two years and may be carried out by CIPSC or by an external entity.

In all audits shall, as a minimum, that the practices of CIPSC and its competent service providers comply with what is established in these Policies, as provided by the administrative authorities and to the provisions of the regulations in force, as well as a methodology that ensures the quality of the services provided.

2.7.- Rates

CIPSC published in the repository mentioned in paragraph 1.6.3 the rates that applied for the provision of each of its services.

CIPSC will not apply any fee for access to the information necessary to verify the

Validity Evidence issued, nor to the present policies and practices statement, or to any of the information that, pursuant to the same, must be made public.

2.8.- Claims and jurisdiction

2.8.1. Communication of the claims

When a signatory, creator of stamps or user part have a claim in respect of the services of CIPSC shall communicate it by any of the means of contact referred to in paragraph 1.6.4 of this document. CIPSC answer to the complaint within a maximum period of one week.

2.8.2. Jurisdiction

The signatories, creators of stamps and users of the services of CIPSC accept the jurisdiction of the courts and tribunals of the city of Zaragoza for any dispute that may arise in connection with the provision of services by CIPSC, expressly renouncing any other jurisdiction that may apply.

3 Statement of Practice

3.1.- Introduction

The operation of CIPSC is based on the technical infrastructure, procedures and control mechanisms that are described in this Statement of practices. Together with the previous chapter, which refers to the policies, regulate the operation and requirements that are common to the various trust services provided by CIPSC.

This document and other information that is relevant to the signatories, creators of stamps and parts users value CIPSC services, are published in the repository as described in paragraph 1.6.3.

The Responsible Policy Management is responsible for maintaining and approve all policies and practices that govern the operation of CIPSC, as well as of the implementation and application of the same. Among other measures, CIPSC performs periodic audits and assessments to determine the state of the controls and safety procedures, carry out the analysis of vulnerabilities and implement such measures as may be appropriate.

Coloriuris, through the Responsible for Policy Management, is responsible for taking the necessary safety measures to comply with the standards and laws, as well as with the policies and practices contained in the present document for the provision of services.

3.2.- The life cycle of certificates

All certificates issued and used by the authorities of CIPSC are in accordance with the standard X.509 version 3 and to RFC 3039*Internet X.509 Public Key Infrastructure Qualified Certificates Profile*".

The identifiers (oids) with RSA encryption algorithms used are the following:

- SHA256RSA: 1.2.840.113549.1.1.11

- SHA512RSA: 1.2.840.113549.1.1.13

The specifications contained in this section are without prejudice to the conditions in each of the Certification Policies for each type of certificate.

3.2.1. Certificate Request

The CIPSC Registration authority receiving the application's responsibility to determine that the requested certificate type is adapted to the specific characteristics of the applicant, in

accordance with the content of the Certification Policy applicable to such certificate and, in this way, resolve the request.

In each certification policy specifies the information that must be provided in advance, to any person who applies for a certificate.

Without prejudice to which it is reported that:

a) The identification of the persons who request a certificate recognized personacion required before the registry operator of the registration authority of CIPSC (or of the R.A. external which may be created in the future) and are accredited by the national identity card, passport or other means admitted in law. Personacion may be waived if your signature on the request for issuance of a certificate recognized has been legitimized in the presence of attorney.

b) In the case of recognized certificates of legal persons (electronic stamps under the name given by R.U.E. 910/2014), the registry operator of the R.A. of CIPSC (or of the R.a. external which may be created in the future) will, in addition, the data relating to the constitution and legal personality and on the extent and duration of the powers of representation of the applicant by means of public documents that serve to accredit the ends referred to reliably and its registration in the corresponding public registry.

3.2.2. Processing the application for certificates.

It is up to the Registration Authority of CIPSC verification of the identity of the applicant, verification of the documentation and the fact that the applicant has signed the document of appearance. Once you complete the application, the Registration Authority shall refer it to the appropriate CIPSC AC.

3.2.3.- Issuance of certificates

CIPSC is not responsible for the monitoring, research or confirmation of the accuracy of the information contained in the certificate after its issuance. In the case of receiving information about the inaccuracy or the non-applicability of the information contained in the certificate, the certificate may be revoked.

The issuance of the certificate will take place after CIPSC has conducted the necessary checks to validate the certification request. The mechanism by which determines the nature and form of such checks is the policy for the provision of certification services.

3.2.4. Acceptance of certificates

The acceptance of certificates on the part of the signatories and/or creators of stamps occurs at the time of the signing of the certification contract associated with each Certification Policy. The Acceptance of the contract implies the knowledge and acceptance on the part of the author and/or creator of stamps of the Certification Policy associated with it.

3.2.5. Use of the key pair and certificate.

The uses of the key pair and certificate are defined by each Certification Policy associated.

3.2.6. Certificate Renewal.

In each of the Certification Policies associated with each type of certificate details the possibility or not to renew the certificates, as well as the conditions for its renewal.

3.2.7.- Key Renewal

The key renewal necessarily implies the renewal of certificate and you will not be able to perform as separate processes.

3.2.8.- Modification of certificates.

You cannot edit the fields of the certificate. Any necessary changes will involve a process of renewal of the certificate.

3.2.9. Revocation and suspension of certificates.

3.2.9.1. Circumstances for revocation

In general, a certificate is revoked when:

- The author/creator of stamps or your keys or keys of your certificates have been compromised by:
  - The theft, loss, disclosure, modification, or other compromise or suspected compromise of the private key of the user.
  - The deliberate misuse of keys and certificates, or the lack of observation of the operational requirements of the underwriting agreement, or of this DPC.
- Faulty occurs the issuance of a certificate due to:
  - That has not been satisfied a prerequisite material for the issuance of the certificate.
  - That a major factor in the certificate is known or reasonably believes that it may be false.
  - A data-entry error or other process error.

- The key pair generated by an end-user is revealed as "weak".
- The information contained in a certificate or used to make your application becomes inaccurate, for example when the owner of a certificate changes its name.
- A valid revocation request is received from an end user.
- A valid revocation request is received from a third party authorised, for example a court order.
- The certificate of a AR or AC above it in the hierarchy of trust certificate is revoked.

While the circumstances for revocation may be specified in each related Certification Policy.

3.2.9.2. Entity that may request revocation

The revocation of a certificate can be encouraged by both the author/creator of stamps as part of CIPSC, as well as by any person who knows that the data associated with the certificate becomes inaccurate or incorrect.

The signatories and creators of stamps can request the revocation of your certificate for any cause and must apply under the conditions specified in the next section.

3.2.9.3. Revocation Request Procedure

The procedure for the application of the reversal of each type of certificate will be defined in the related Certification Policy.

3.2.9.4. Grace period for Revocation Request

The revocation will take place immediately to the processing of each request not verified as valid. Therefore there is no grace period associated with this process.

3.2.9.5. Circumstances for suspension

The suspension implies the invalidity of the certificate during the time that remains suspended. The suspension can only be declared if so decided by a judicial or administrative authority, by the time that the same set. CIPSC does not support the suspension of certificates as an independent operation on their certificates.

3.2.9.6. Entity that may request the suspension

The suspension can only be requested by a judicial or administrative authority.

3.2.9.7. Procedure for the application of suspension

The suspension of a certificate shall be requested by judicial or administrative order.

3.2.9.8. Limits of the suspension period

Establish the competent judicial or administrative authority.

3.2.9.9. Frequency of CRLs

CIPSC will publish the CRL's of your AACC in your repository each 30 days provided that there has been no revocation, in the event of a revocation, the corresponding CRL will be issued immediately, without prejudice to the fact that this revocation can be known also by OCSP.

3.2.9.10. Requirements of certificate status check

The verification of the status of the certificates is required for each use of the certificate of end entities. This verification can be done through the OCSP protocol that provides CIPSC indicated in paragraph 4.2.1.5.

In addition, CIPSC also contemplates the publication of CRLs.

3.2.9.11. Other forms of dissemination of revocation information available

CIPSC reserves the right to introduce in the future other forms to report the revocation of certificates.

3.2.9.12. Special requirements of key renewal committed

There is no variation in the previous clauses when the revocation is due to compromise of the private key.

3.2.10. Services certificate status check.

3.2.10.1. Operational Characteristics

CIPSC offers a free publication of certificate revocation lists (CRLS) without access restrictions. In addition, offers services of validation of certificates using the OCSP protocol.

The OCSP service is available for all the certificates issued by the CIPSC's authorities. The issued responses by the OCSP service are authenticated by special certificates issued by the respective CIPSC's authorities with this sole purpose.

3.2.10.2. Service Availability

The CRLs and OCSP online consultation of the status of the certificates are available during the 24 hours a day, 7 days a week.

May be scheduled service interruptions when strictly necessary for technical reasons, in which case these must be announced at least 24 hours in the directory indicated in section 1.6.3.

When the interruption is due to causes of force majeure or serious incident, CIPSC will act with the utmost diligence to achieve the implementation of the services, as well as to minimize the potential harms that have been caused to the signatories, creators of stamps and/or parts users

3.2.11. Completion of the subscription.

The Subscription ends with the expiry or revocation of the certificate.

3.2.12. Deposit and key recovery.

CIPSC does not offer that service.

3.3.- Physical security controls, procedural and staff

3.3.1. Physical Security Controls

3.3.1.1. location and construction of facilities

The facilities in which is processed the information provided they meet the following requirements: Physical

- The building that contains the information processing facilities is physically solid, the outside walls of the site are of solid construction and is permanently monitored by security cameras, allowing only the access to duly authorized persons.
- The processign Chamber has its doors closed and protected against unauthorized access and has no windows.

3.3.1.2. Physical Access

Facilities include a system of physical access control:

- Access is allowed only to authorized personnel.
- The rights of access to the secure area are reviewed and updated regularly.
- It is required that all staff porte some element of visible identification and encourages the staff requiring such identification to anyone who does not have the same.
- The personnel belonging to the operation of CIPSC working on their facilities is supervised.
- Securely maintained a file of the access according to ISO 27001.
- The entrance doors are equipped with access mechanisms.
- A closed-circuit television monitors the room room from which the service is provided.

3.3.1.3.- Electricity and air conditioning

The Data Center with energy systems and air conditioning to ensure a reliable operating environment.

The facilities have a functionality of uninterruptible power supply (UPS) that keeps the equipment in operation during the time required for the orderly closure of the systems in the event of a power failure or air conditioning will cause its fall.

3.3.1.4. exposure to water

The necessary measures have been taken to minimize the risks arising from water damage.

3.3.1.5. Prevention and fire protection

The Data Center has automatic fire detection systems with the aim of:

- Warn of a fire to guard service and staff.
- Comply with the missions of disconnection of the ventilation system, court of electrical energy and the shooting of the automatic installation of extinction.

3.3.1.6. Media Storage

The backups are stored securely .

3.3.1.7. Treatment of waste

The media containing confidential information are destroyed in such a way that the information may not be able to recover after its destruction.

3.3.1.8. Backup offsite

CIPSC stores the backups that are protected against accidents and at a sufficient distance to prevent them from being damaged in the event of a disaster in the main site.

3.3.2. Procedural Controls

3.3.2.1.- Functions Reliable

Is defined: "the role of confidence" as that to which the assigned functions that can lead to security problems if not properly carried out, either by accident or Malicious.

With the purpose of increasing the likelihood that the duties corresponding to a "role of trust" are performed correctly, there are two approaches:

- The first is the design and configuration of the technology, in such a way as to avoid mistakes and improper behavior is prohibited.

- The second is the distribution of functions between several people in such a way that the malicious activity requires the connivance of several of them.

As specified in the standard CEN CWA 14167-1, the minimum roles are:

- **Responsible for Security (Security Officer):** holds the overall responsibility for the administration and the implementation of safety policies and procedures.
- **Administrators of the certification system (System Administrators):** authorized to make changes to the system configuration.
- **System operators (System Operator):** Responsible for the day-to-day management of the system (monitoring, backup, recovery,…)
- **Internal Auditor (System Auditor):** authorized to access the system logs and verify the procedures that are performed on the same.
- **AC Operator - Operator Certification :** Responsible for activating the CA keys in the online environment.
- **AR operator (Registration Officer):** Responsible for approving, to issue, suspend and revoke the end entity certificates.

Specifically:

The tasks of Auditor are incompatible in time with the certification tasks and incompatible with systems.

The people involved in Systems Management may not engage in any activity in the tasks of audit or certification.

3.3.2.2. Number of people per task

To strengthen the security of the system, are assigned different people for each role with the exception of the role of operator that can be assumed by the administrator.

In addition, you can assign multiple individuals to the same role.

3.3.2.3. Identification and authentication for each role

The Trusted roles require authentication with a sufficiently secure, and in any case always with personal users.

3.3.2.4. Separation of tasks in the different roles

The people assigned for each role are identified by the internal auditor to ensure that each person carries out the operations for which it is assigned.

Each person only controls the assets necessary for your role, ensuring that no person access to resources that are not allocated.

3.3.3. Personal controls

3.3.3.1. Requirements of history, qualifications, experience and authentication

CIPSC employs staff who possesses the experience and qualification needed for the services to be performed.

All of the staff roles reliable is free of interests which might impair the impartiality of CIPSC operations.

3.3.3.2. Investigation Procedures of history

Does not apply according to the Spanish legislation.

3.3.3.3. Training Requirements

The CIPSC staff receive the training required to ensure their competence in the performance of its functions. The training is included in the following points:

- Delivery of a copy of the Declaration of Certification Practices.
- Security awareness.
- Operation of the software and hardware for each specific role.
- Security procedures for each specific role.
- Procedure of operation and management for each specific role.
- Procedures for disaster recovery.

3.3.3.4. Requirements and frequency of update training

In the face of technological changes in the environment, introduction of new tools or modification of operating procedures, take the appropriate training for the staff concerned.

In the face of changes in the Declaration of Certification Practices, Certification Policies and other relevant documents, shall be carried out training sessions.

3.3.3.5. Sequence and frequency of job rotation

Not applicable.

3.3.3.6. Sanctions for unauthorized actions

In the case of commission of an unauthorized action with respect to the operation of the Certification Authority disciplinary action will be taken. Be considered unauthorized actions which contravene the Declaration of Certification Practices or policies of the relevant certification both negligent as malicious.

If there is any infringement, CIPSC shall suspend the access of the people involved to all systems of CIPSC information immediately to the knowledge of the fact.

In addition, depending on the seriousness of the offenses, the penalties provided for in the collective agreement for the company, or the status of the workers as appropriate to the employment situation of the offender.

3.3.3.7. Requirements of recruitment of staff

CIPSC said that complies with the regulations in force in the field of equal opportunities between men and women, and that also has an active policy in this regard.

CIPSC undertakes to ensure that all staff seconded to the services know, assume and

To comply with the obligations of this Policy and Disclosure Practices in the form and manner of its compliance, security and confidentiality, that will be extended to all those involved in the processes, treatments, and implementation of the certification work, constituting its code of ethics. To this end CIPSC undertakes to obtain from each one of your employees and partners a written commitment in this regard.

CIPSC declares to know the principles of the United Nations Global Compact, assuming its full content and committing to their strict enforcement.

In relation to the allocation of roles and responsibilities shall be subject to the provisions of paragraph 3.3.2.1.

3.3.3.8. Provision of documentation to the staff

All personnel involved in roles reliable receives:

- A copy of the Declaration of Certification Practices
- The documentation that defines the obligations and procedures of each role.
- You have access to the manuals relating to the operation of the different components of the system.

3.3.4. Log and audit procedures

Use the log files to reconstruct the significant events that have been carried out by the software used by CIPSC and registration and the user or event that gave rise to them. It will also be used as a means of arbitration in disputes by checking the validity of a signature in a given time.

3.3.4.1. Type of events recorded

Are stored in the logs:

- All events related to the life cycle of the cryptographic keys.
- All events related to the life cycle of the certificates.
- All events relating to the issue of cryptographic devices.
- All events relating to the administration of accounts of CIPSC operators and managers.

Date and time of each event is recorded, using a reliable time base.

3.3.4.2. Frequency of processing logs

Log files are periodically reviewed by the auditor of CIPSC.

3.3.4.3. retention period for the log

The information generated in the log file is kept in line until the moment of being filed. Once filed, the log files are maintained for 7 years.

3.3.4.4. Protection of the log

Is assigned to the Auditors the right reading log.

This prevented unauthorized deletion of log records and the modification of the same, by writing log records to a non-editable as a CD-ROM or other.

3.3.4.5. the log backup procedure

Backups of the log in line with the same planning and controls that for the rest of elements of the system of CIPSC.

3.3.4.6. Collection of logs

The log files of AACC and ARRA are stored in the internal systems of CIPSC.

3.3.4.7. Notice of the action causing the logs

It is not referred to the notice of the action of the log files to the source of the event.

3.3.4.8. Analysis of vulnerabilities

There is a periodic vulnerability scanning in the internal systems of CIPSC.

3.3.5.- Archive of records

3.3.5.1. Type of archived records

The types of data or files that are archived, among others, are the following:

- Data related to the procedure of registration and certificate request;
- The audit records from the previous section;
- Key Historical

3.3.5.2. The file retention period

All the information and documentation relating to the certificates shall be kept for 15 years (from the date of issuance).

3.3.5.3. Protection of the file

Measures shall be taken for the protection of the file, so that it cannot be tampered with or destroyed its contents.

3.3.5.4. The file backup procedures

There is a backup policy, Plan of Contingency and business continuity plan that define the criteria and strategies for action before an incident. The design of the entire incident action strategy is based on the corresponding asset inventory and risk analysis.

3.3.5.5. Requirements for the sealing of records

The information systems employed by CIPSC guarantee the registration of the instants of time in which it was made. The time of the systems comes from a safe source of date and time. All systems synchronize their time with this source.

3.3.5.6. File System

The file system is housed in the premises of CIPSC and in the entities involved in the provision of the service.

3.3.5.7. Procedures for obtaining and verifying the information in the file

Access to this information is restricted to authorized personnel to that effect, protecting against physical and logical access as set out in other sections of 3.4 and 3.5 section of the present Declaration of Certification Practices.

3.3.6. Change of keys

To renew a certificate of user, either because it has been revoked or has expired, you must request a new certificate, following the process of issuance of certificates provided for in the specific documentation for each certificate.

The key renewal goes hand in hand with the renewal of the certificate.

3.3.7. Contingency Plan

3.3.7.1.- Incident Management Procedures

There is a contingency plan that defines the activities to be carried out, resources to use and staff to use in the event of a malicious or accidental event that disable or degrade resources and certification services provided by CIPSC.

The main objectives of the Contingency Plan are:

- Maximize the effectiveness of the recovery operations through the establishment of 3 phases:
  - Notification stage/Evaluation/Activation to detect, assess the damage and to activate the plan.
  - Recovery Phase to restore temporarily and partially services until the recovery of the damage caused in the original system.
  - Phase of reconstruction to restore the system and operational processes to their usual.
- Identify the activities, resources and procedures necessary for the provision of certification services in a CPD alternative during prolonged interruptions of the normal operational.
- The allocation of responsibilities to designated staff CIPSC and provide a guide for the recovery of the usual operating for long periods of interruption.
- Ensure the coordination of all the actors (departments of the entity, external points of contact and sellers) to participate in the contingency strategy planned.

The Contingency Plan of CIPSC is of application to the set of functions, operations and resources needed to restore the provision of certification services. This plan applies to the CIPSC staff associated with the provision of certification services.

The Contingency Plan establishes the participation of certain groups in the recovery of operations of CIPSC.

The evaluation of the damage and the plan of action are described in the Contingency Plan.

In the case of the fact that the algorithm, the combination of the key sizes used or any other circumstance technique that significantly impair the safety of the system will apply the Contingency Plan. There will be an impact analysis. Such an analysis should consider the criticality of the security problem, its scope and the recovery strategy before the incident. The points that must be defined as a minimum in the report of impact analysis are:

- Detailed description of the contingency, temporal scope, etc
- Criticality, field

- Solution or solutions proposed
- Plan for the deployment of the solution chosen, which will include at least:
  - Notification to the users by the means considered more effective. It will include both applicants and the signatories, creators of stamps and verifiers (third parties) of the certificates.
  - The information shall be submitted to the web site of the contingency produced
  - Revocation of certificates affected
  - Renewal Strategy

3.3.7.2. Plan of action to corrupt data and software

If the resources hardware, software, and/or data is altered or are suspected of having been altered will stop the operation of the CIPSC services until the restoration of a safe environment with the addition of new components of efficiency creditable coverage. In parallel will conduct an audit to identify the cause of the alteration and ensure no reproduction of the same.

In the case of affected certificates issued, it shall notify the fact to the signatories, creators of stamps of the same as well as Minetur and proceed to your recertification.

3.3.7.3. Procedure Before compromise of the private key

The Root CA will revoke the certificate from a CA subordinate in the case that the private key of the CA has been compromised.

In the case that the Root CA must revoke the subordinate CA certificate, it shall forthwith:

- The AC radio station
- All the ARRA authorised for the registration of that AC
- All signatories to the holders of certificates issued by that AA.
- Ministry of Energy and Tourism and Digital Agenda of Spain.

The Root CA, will also publish the revoked certificate in the ARL/CRL (Certificate Revocation List of Certification Authorities).

After you resolve the factors that led to the revocation, the root CA, you can:

- Generate a new certificate for the subordinate CA.
- Ensure that all new certificates and CRLS issued by the AC are signed using the new key.

The AC subordinate may issue certificates to all end entities affected.

In the event that the compromised key of the root CA, the certificate of all applications and distributed a new one.

3.3.7.4. Business Continuity after a disaster

We will suspend the operation of the AC until the time when it is completed the disaster recovery procedure and is working properly in the primary or alternate center.

Will the Plan of Contingency and Business Continuity of CIPSC.

3.3.8. Termination of the AC or AR

3.3.8.1. Certification Authority

In the event of termination of his activity, CIPSC communicated to the signatories and creators of stamps by any means that guarantees the sending and receipt of the notification, with a minimum period of 2 months in advance of the date of its extinction, its intention to cease as a provider of certification services.

In the same way, shall be notified to lhp and any entity with which CIPSC keep any contractual relationship of use of your certificates.

It was also communicated to the Ministry of Energy and Tourism and Digital Agenda of Spain, with the notice referred to in the previous paragraph, the cessation of their activity and the destination you go to give the certificates, specifying, in your case, if you are going to transfer the management and to whom or if you cease to be valid.

The responsibility of this notification applies to the Security Responsible of CIPSC, who will decide the most appropriate mechanism.

In the course of that CIPSC decide to transfer the activity to another provider of certification services, shall notify the Ministry of Energy and Tourism and Digital Agenda of Spain and the signatories and creators of stamps of their certificates the transfer agreements. To this end CIPSC sent the explanatory document to the terms of transfer as well as the conditions of use which govern the relations between the signatories and/or creators of stamps and the PSC to which transfer the certificates. This notification shall be made by any means that guarantees the sending and receipt of the notification, with a minimum of 2 months to the cessation of their activity.

The signatories and creators of stamps must expressly consent to the transfer of the certificates, accepting the terms of the PSC to which the goods are to be transferred. After the

period of two months, and there is no transfer agreement or without the signatories and creators of stamps expressly accept the same, the certificates will be revoked.

On the assumption that there were no agreements with other PSC, completed within the last 2 months in advance in the communication, all certificates will be revoked automatically.

CIPSC forwarded to the Ministry of Energy and Tourism and Digital Agenda of Spain, prior to the termination of its activity the information relating to the electronic certificates whose validity has been extinguished to take charge of their custody for the purposes of article 20.1.f).

It will be terminate any third party authorization with the CIPSC that hold a contract for the provision of services (identification, issue, etc.)

3.3.8.2. Registration Authority

Once the Registration Authority ceases in the exercise of the functions that take will transfer the records to keep CIPSC, while there is no obligation to maintain filed the information given in another case, will be canceled and destroyed.

3.4.- Technical Security Controls

3.4.1. Generation and installation of the key pair

CIPSC adopts the measures needed to ensure that the private keys of its authorities are secret and to maintain its integrity.

3.4.1.1.- Generating the key pair

Elements where the key pair is generated for each of the different entities that make up CIPSC:

- AC root: the machine where lies the root CA has a cryptographic device (HSM) for key generation of the root CA.
- AACC subordinate: it must generate a cryptographic module on every machine that hostel AACC.
- User certificates issued in cryptographic card or HSM: The keys are generated by the cryptographic device.
- User certificate issued in cryptographic software support: Your keys are generated by the server where the service resides

- Server Time Stamping Authority (TSA) and OCSP validation Server: keys generated in the cryptographic module associated with the system in which they reside both servers.
- In the case of the keys generated by the holder, these must be generated following the recommendations of algorithm and key length minimum standards defined in ETSI TS 102 176

3.4.1.2. Distribution of the private key of the signer or creator of Seal

Delivery method of the private key for the different entities that make up or collaborate with CIPSC:

- Certificates issued in cryptographic card: the private key authentication and signature are delivered with the cryptographic device.
- Certificates issued in HSM: private keys for authentication and signature are housed in the cryptographic device.
- Certificates issued in software support: the private key is generated on the server itself. You do not need to be delivered.

3.4.1.3. Distribution of the public key to the issuer of the certificate

The method of delivery of the public key of the different entities that make up or collaborate with CIPSC corresponding to the issuer of certificates is the following:

- AACC subordinate: the public key is sent to the root CA using X.509 or PKCS#10.
- Certificates issued in cryptographic device: cryptographic device is read.
- Certificate issued in software support: The public key is sent to the AC of CIPSC through X.509 or PKCS#10.

3.4.1.4. Distribution of the public keys of the authorities providing services

The public keys of the authorities providing services will be published, as well as their chain of trust, through the respective electronic certificates in the repositories as described in paragraph 1.6.3 of this document. The format of the certificates shall be as defined by the standard X509 v3, and its content, and period of validity which may be determined by the corresponding policies.

In the present Declaration of Certification Practices, in Annex II, shall be published in addition to the different tracks of the AACC roots and AACC subordinate.

3.4.1.5. Key Sizes

The size of the keys, depending on the cases is:

- At least 2048 bits for natural and legal persons, OCSP server, server TSA and technical certificates.
- At least 2048-bit keys of AACC subordinate.
- At least 4096 bits for root keys of AC.

If it is determined that any of the key lengths have ceased to provide an adequate level of security, CIPSC The replaced by other whose security level is deemed sufficient, and publish the information on these changes in the repository mentioned in section 1.6.3.

3.4.1.6. Certificate Signing Algorithms

The algorithm identifier (CIPSC AlgorithmIdentifier) that uses to sign certificates is SHA-256 (a hash algorithm) with RSA signature algorithm) that corresponds to the identifier for "Secure Hash Algorithm (SHA256 256) with Rivest, Shamir and Adleman (RSA) encryption".

The end-user certificates are signed with RSA with SHA-256. CIPSC recommends to end users who use RSA with SHA-256 or higher at the time of signing with the certificate.

CIPSC uses an algorithm qualified by the industry and suitable for the purpose of signature recognized. To be taken into account for the period of validity of the certificate in addition follows the recommendations indicated by the different standards of ETSI.

In the case of the fact that the algorithm, the combination of the key sizes used or any other circumstance technique that significantly impair the safety of the system will apply the Contingency Plan. There will be an impact analysis. Such an analysis should consider the criticality of the security problem, its scope and the recovery strategy before the incident. The points that must be defined as a minimum in the report of impact analysis are:

- Detailed description of the contingency, temporal scope, etc
- Criticality, field
- Solution or solutions proposed
- Plan for the deployment of the solution chosen, which will include at least:
  - Notification to the users by the means considered more effective. It will include both applicants and the signatories, creators of stamps and verifiers (third parties) of the certificates.
  - The information shall be submitted to the web site of the contingency produced or revocation of certificates affected
  - Renewal Strategy

3.4.1.7. Supported Uses of keys (KeyUsage field X.509v3)

All certificates include the extension Key Usage and Extended Key Usage, indicating the uses enabled the keys.

The keys of root CA will only be used to sign certificates of AACC ARLs and subordinate, and that the keys of the AC or subordinate stations will be used only to sign end-user certificates and CRLs

The supported uses of the key for each certificate are defined in the specific section of each certificate.

3.4.2. Protection of the private key

3.4.2.1. Standards of cryptographic modules

A cryptographic security module (HSM) is a security device that generates and protects cryptographic keys. CIPSC uses cryptographic hardware modules developed by third parties and are commercially available. CIPSC only uses cryptographic modules with FIPS 140-2 Level 3 Certification, CC EAL 4+ or higher.

CIPSC verifies that the cryptographic security modules have not been tampered with during transportation and storage, and retain the original packaging factory.

In terms of the cryptographic devices with certificates for a qualified electronic signature, allergy-free devices as secure signature creation (cam 3.11.10), meet the security level of the CC EAL4+, although they are also admissible the equivalent certificates ITSEC E3 or FIPS 140-2 Level 2 as a minimum.

The European standard of reference for devices of signatories or creators of stamps used is CEN CWA 14169.

CIPSC, in any case, maintains control over the preparation, storage, and distribution of the devices of the signatories and creators of stamps in the CIPSC that generates the keys.

3.4.2.2. Control by more than one person (n m) on the private key

The use of the private keys of the AACC requires the approval of at least two people.

3.4.2.3. Custody of the private key

The private key of the AACC root are guarded by a cryptographic hardware device certificate with the FIPS 140-2 Level 3 and/or CC EAL4+, ensuring that the private key is never outside the cryptographic device. The activation and use of the private key requires the control multipersona detailed above.

The private keys of the AC subordinates are guarded in cryptographic devices insurance certificates with the FIPS 140-2 level 3 and CC EAL4+.

In the cases in which the author or creator of stamps watch over the private key, this will be the responsible for maintaining it under their exclusive control.

3.4.2.4. Backup copy of the private key

In order to ensure continuity of service in the event of a total disaster (destruction of the HSM that holds the private keys of the root certificates) there is a backup in a secure signature creation device of the same characteristics as the HSM in production.

The backup has been carried out by the Administrator of the Certification System and the Operator of the Certification Authority, under the supervision of the Safety Officer, in accordance with the provisions of section 3.4.2.2, which retains such backup in A safe enough distance from the main site.

3.4.2.5. Archive of the private key

CIPSC not to close the private signature key certificate after the expiration of the period of validity of the same.

The private keys of the internal certificates that use the different components of the system of the AC to communicate among themselves, sign and encrypt the information may be filed after the issuance of the last certificate.

The private keys of the signatories and creators of stamps may be filed by themselves through the conservation of signature creation device or other methods, because they may be needed to decrypt information encrypted with the public key, provided that the device of custody to permit the operation.

3.4.2.6. Transfer of the private key to or from the cryptographic module

Only in the event of a contingency is used the procedure referred to in paragraph 3.4.2.4, which is described in the contingency plan, to retrieve the private key in the cryptographic modules.

3.4.2.7. Storage of the private key in the cryptographic module

The private keys, both of the AACC as AACC subordinate are generated directly within the cryptographic module that will house. CIPSC continues for the generation of the keys of the AACC the recommendations of ETSI TS 101 456, 7.2.1.

In cases where private keys are stored outside of the cryptographic modules, these will be protected in a way that ensures the same level of protection as if they were physically in the interior of the cryptographic modules.

3.4.2.8. Activation method of the private key

The keys of the Root CA and the AACC subordinate are activated by a process that requires the simultaneous use of n m cryptographic devices.

Access to the private key of the signer or creator of stamps is carried out by means of a pin. The device has a system of protection against attempts to access blocking it when more than three times a wrong access code. The author or creator of stamps has an unlock code of the device. If it is entered incorrectly three times, your device is permanently locked, it being unusable.

3.4.2.9. Deactivation method of the private key

An administrator can deactivate the key CIPSC authorities through the procedure provided by the system of the HSM.

In the case of the author or creator of stamps, the removal of the reader's cryptographic device involves the termination of any action of operation in progress.

3.4.2.10. Method of destruction of the private key

The manual of the HSM provides a secure method of destruction of keys of the AC. In the case of remove the HSM that holds the keys of the AC, these will be destroyed.

This procedure does not apply to the signing keys or user authentication issued in cryptographic card except, in the case of key renewal by reusing the same cryptographic device, which will destroy the previous key and generate new keys on the same media.

3.4.2.11. Qualification of the cryptographic module

As indicated in paragraph 3.4.2.1 of this document

3.4.3. Other aspects of management of the pair of keys

3.4.3.1. Archive of the public key

The certificates generated by the AC, and therefore the public keys are stored by the AC during the period of time required by the legislation in force.

3.4.3.2. Periods of use of public and private keys

Is the period of validity of each one of the certificates.

3.4.4. Activation Data

3.4.4.1. Generation and data installation of activation

- For the certificates from the AC, the activation data are generated in cryptographic tokens in possession of authorized personnel,

- Certificates issued in cryptographic device: the use of the private key associated with each certificate requires an activation data (PIN) or password.

  The activation data (PIN) or password:

  - Is randomly generated by the software of CIPSC and is recorded in the cryptographic device that supports the certificate.
  - It generates and prints at the time of issue of the certificate.
  - Is delivered to the user by a system that allows you to maintain confidentiality.
  - CIPSC provides the signer or creator of stamps a function for changing your PIN on the card.
  - The PIN is never stored.

- Certificates issued in support software: the installation and commissioning of the private key associated with the certificate requires the use of the security systems that the user has defined.

3.4.4.2. Protection of activation data

In relation to the activation data signature is required to users of certificates:

- Memorizing them.
- Use the maximum care to protect them.
- Do not store them next to the cryptographic device or share them with other people.
- Change the PIN and PUK before use

3.4.4.3. Other aspects of the activation data

Does not provide for the life time of the activation data. However, it is recommended that you change them periodically to reduce the possibility that they are discovered.

3.4.5. Computer Security Controls

3.4.5.1. Specific technical requirements of computer security

There are a series of controls in the location of the different elements of the service delivery system of certification of CIPSC (AACC, database of CIPSC, CIPSC Internet Services, Operation and Management of Network):

- Operational Controls.

- Documenting the processes of operation by the operator of the A.C. And the administrator of the security system in accordance with manufacturer's manuals of the HSM.

  There is a Contingency Plan.

- They are installed tools of protection against viruses and malicious code.
- A continued maintenance of the equipment, in order to ensure continuous availability and integrity.
- The information of the obsolete information media and removable media is deleted; the teams are tagged and delivered to the responsible for security that are kept in a safe place until its destruction by specialized companies.

- Data exchanges. The following exchanges of data are encrypted to ensure confidentiality.
  - Registration data transmission between the ARRA and the registration database.
  - Pre-registration data transmission.
  - The communication between the ARRA and the AACC.
- The CRL publishing service has the features necessary to ensure 24x7 operation.
- Access Control.
  - Use unique user IDs, so that users are related to the actions carried out and cannot be held responsible for their actions.
  - The allocation of rights is carried out according to the principle of granting the minimum privileges.
  - Immediate removal of the access rights of the users who change jobs or leave the organization.
  - Quarterly review of the access level assigned to users.
  - The allocation of special privileges is made "on a case-by-case basis" and are deleted once the cause of your assignment.

3.4.5.2. Evaluation of the level of computer security

The safety of the equipment is reflected by an initial risk analysis in such a way that security measures are a response to the probability and impact occurred when a group of threats defined to take advantage of security breaches as described in the plan of contingency and business continuity.

Physical security is guaranteed by the facilities already defined above and the management of staff.

3.4.6. Technical controls of the life cycle

3.4.6.1. Controls Systems Development

An analysis is made of the security requirements during the phases of design and specification of requirements of any component used in the application of certification authority and

Registration Authority, to ensure that the systems are safe. Used change control procedures to the new versions, updates and patches of emergency, of those components.

3.4.6.2. Management controls of the security

CIPSC maintains an inventory of all assets and perform a classification of the same in accordance with their protection needs, consistent with the risk analysis carried out.

The configuration of the systems is audited on a regular basis, in accordance with the appropriate section of this document.

The CIPSC systems are protected against viruses and unauthorized and malicious software.

Track of capacity needs is followed, and will be planned procedures to ensure adequate availability and storage for informational assets.

3.4.7. Network Security Controls

Ensures that the access to the different networks of CIPSC is limited to individuals duly authorized. In particular:

- Are implemented controls (such as firewalls) to protect the internal network from external domains accessible by third parties. Firewalls are configured in such a way as to prevent unauthorized access and protocols that are not required for the operation of the CIPSC.
- Sensitive data is protected when it is exchanged over non-secure networks (including the registration data of the author/creator of stamps).
- This ensures that the local network components (such as routers) are located in secure environments, as well as the periodic audit of your settings.

3.4.8. Time Source

CIPSC gets the time of their systems of a connection to the Royal Observatory of the Navy following the NTP protocol. The description of the NTP protocol can be found in the IETF standard RFC 5905.

Annex I

Acronyms used

- **AC:** Authority of CIPSC for the provision of trust services
- **AR:** Registration Authority
- **ASD:** Authority of CIPSC for the provision of services relating to electronic documents
- **CEN-CWA:** Committee européen de normalisation - CEN Workshop Agreement
- **CIPSC:** Coloriuris Provider of Trust Services
- **CN:** Common Name (Common Name). Attribute of the Distinguished Name (DN) of an object within the X.500 directory structure
- **CRL:** Certificate Revocation List (CRL)
- **Cam 3.11.10**: Secure Signature Creation Device
- **EAL:** Evaluation Assurance Level
- **ETSI:** European Telecommunications Standard Institute
- **FIPS:** Federal Information Processing Standard (Standard uses of information processing)
- **HSM:** Hardware Security Module. Security module used to store cryptographic keys and cryptographic operations in a safe manner.
- **IETF**: Internet Engineering Task Force (Internet standardization body)
- **OASIS:** Organization for the Advancement of Structured Information Standard
- **OCSP**: Online Certificate Status Protocol. This protocol allows check online the validity of an electronic certificate.
- **OID**: Object Identifier (OID)
- **PKI**- Public Key Infrastructure (Public Key Infrastructure)
- **PSC**: Provider of Trust Services
- **RFC**: Request For Comments (Standard issued by the IETF)
- **SSCD:** Secure Creation Device (Secure Signature Creation Device)
- **TSA**: Time-stamping authority (Time Stamping Authority)

- TSACI: Authority of CIPSC for the provision of the service of time stamping
- **TST**: Time-stamping Token (Time Stamp)
- **TSU**: Time-stamping Unit (Time Stamping)
- **UTC**- Coordinated Universal Time (Coordinated Universal Time)
- **XadES:** XML Advanced Electronic Signature

Definitions

- **Authorities CIPSC services:** are the authorities who provide each of the services of trust CIPSC
- **Certificate of electronic signature:** An electronic statement that links the data validation of a signature with a physical or legal person and confirms, at least, the name or pseudonym of that person;
- **Certificate of electronic stamp:** a statement that links the data validation of a stamp with a legal person and confirms the name of that person.
- **Key Login**: password that is generated specifically for a communication or meeting, ending its usefulness after this.
- **Public key and private key**: the asymmetric cryptography uses a pair of keys in which what is encrypted with one of them can only be decrypted with the other and vice versa, to one of these keys is called public (matches the signature creation data electronics) and it is included in the electronic certificate, while the other is private and is only known by the holder of the certificate.
- **Identification data of the person:** a set of data that allows you to establish the identity of a natural or legal person, or a person who represents a legal entity;
- **Validation data:** the data used to validate an electronic signature or an electronic stamp.
- **Practice Statement**: Statement of the practices that an authority used for the provision of their services.
- **Electronic document:** all content stored in electronic format, in particular, text or sound recording, visual or audiovisual.
- **Evidence:** Are the authentic elements issued by the CIPSC. These include, in particular, the electronic certificates, the time stamps and certificates of emission and reception of electronic certificates and, in general, any electronic document authentic is issued as a result of the provision of a service of trust CIPSC and expressly contemplated in these policies and practices.
- **Electronic Identification:** The process of using the identification data of a person in an electronic format that represent a unique way to a natural person or legal entity or a natural person representing a legal person;

- **Time stamping policy**: a set of rules that govern the applicability of the time stamp and their emission characteristics.

- **The certification services provider: any** natural or legal person who issued electronic certificates or provides other services in connection with the electronic signature.

- **Provider of trust services:** a natural or legal person that provides one or more services of trust, as well as provider qualified or non-qualified personnel as a provider of services of trusts.

- **Electronic time stamp:** data in electronic format that link other data in electronic format with a specific moment, providing proof that the latter data existed at that moment.

- **Time stamp**: structure of data on some data that link to a particular moment in time, providing evidence of its existence prior to that moment.

- **Electronic Stamp:** data in electronic form which are annexd to other data in electronic format, or logically associated with them, in order to ensure the authenticity and integrity of the latter.

- **Service of trust:** the electronic service provided normally provided for remuneration, consisting of: the creation, verification and validation of signatures, electronic stamps or electronic time stamps, electronic delivery services certified and certificates relating to these services, or the creation, verification and validation of certificates for authentication of web sites, or the preservation of signatures, stamps or electronic certificates relating to these services.

- **Certified electronic delivery service:** a service that allows you to transmit data between third parties by electronic means and provides evidence relating to the management of the data transmitted, including proof of sending and receiving data, and which protects the data transmitted from the risks of loss, theft, damage or unauthorized alteration.

- **Author:** Natural person who creates an electronic signature.

- **Creator of stamp:** legal person that creates an electronic stamp.

- **Part Client**: natural or legal person who trusts in the electronic identification or the trusted service.

- **Coordinated Universal Time (UTC):** time scale, based on the second, as defined by the Committee of Radio of the International Telecommunication Union (ITU-T) TF.460-5.

- **Togetherd time-stamping Time-Stamp Unit (TSU): a** set of hardware and software that is managed as a unit and that has a single private signature key is active at any one time.

- **Validation:** The process to verify and confirm 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 to the development and/or application of the present policies and practices statement of Coloriuris Provider of Trust Services:

- *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates V1*
- *CA/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 administration of policies of Coloriuris S.L.

Date: April 9, 2018

Anex II. Policy Review

Theese 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.