ECD_CO_1001_Certification Practice Statement

Lleida SAS

Colombia- Bogotá

Content

1 DOCUMENTARY CONTROL

This section reflects the document information, its properties and version history.

1.1 History of versions

Version	Date	Author	Description
1	30/07/2021	Eva Pané	Initial version
2	03/03/2022	Gloria Salvador	Incorporation of PKI services
3	17/06/2022	Gloria Salvador	PKI improvements
4	13/12/2022	Gloria Salvador	Amendment of certificates
4.1	03/05/2023	Gloria Salvador	ONAC accreditation references
4.2	19/9/2023	Gloria Salvador	Wording Improvements

1.2 Distribution list

Company
Lleida SAS

1.3 Classification and status

Classification	Status
Internal Use	Approved

1.4 Documents r eferenced

Description

2 INTRODUCTION

2.1 Preliminari considerations

The **Certification Practices Statement** (hereinafter, CPS or DPC in Spanish) is a document prepared by LLEIDA SAS, (hereinafter LLEIDA.NET), acting as Digital Certification Entity (hereinafter ECD), contains the rules, statements on policies and procedures that the ECD as Digital Certification Service Provider (CSP) applies as guidelines to provide digital certification services in accordance with the provisions of Law 527/1999, Decree 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, in the territory of Colombia.

The CPS is in accordance with the following guidelines:

i. Specific Accreditation Criteria for Digital Certification Entities CEA-3.0-07 Version 2 (hereinafter CEA) that must be fulfilled to obtain the Accreditation as Digital Certification Entity-ECD, before the National Accreditation Body of Colombia- ONAC.

ii. The DPC is organised under the structure defined in RFC3647 Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework of the IETF-The Internet Engineering Task Force (which replaces RFC2527).

The updating and/or modification of the CPS shall be carried out through the procedure established by LLEIDA.NET for documented information; any change or adaptation to the document must be reviewed, analysed and approved by the Security Committee.

DATOS DE LLEIDA S.A.S.:

Company name:	LLEIDA S.A.S.
N.I.T.	900571038-3
Address:	Calle 81 # 11 - 55 Office 903, Bogotá D.C.
City/Country	Bogotá/Colombia
Telephone:	+5713819903
E-mail:	co@lleida.net
Website:	www.lleida.net/co
Accreditation Certificate No.	22-ECD-009
Accreditation Certificate	22-ECD-009.pdf (onac.org.co)

2.2 Requests, complaints, claims, requests and appeals

Requests, complaints, claims, requests and appeals about the services provided by LLEIDA.NET or subcontracted entities, explanations about this CPD and its policies; are received and dealt with directly by LLEIDA.NET as ECD and will be resolved by the relevant and impartial persons or by the committees that have the necessary technical competence, for which the following channels are available for the attention of subscribers, responsible and third parties.

Telephone: +57 (1) 3819903
E-mail: clientes@lleida.net
Website: www.lleida.net/co
Responsible: Customer Service Area

Once the case is presented, it is forwarded with the relevant information to the Customer Service area according to the internal procedure established for the management of these issues, and once the complaint is received, it is followed up to provide a timely response to the customer.

Once the PQRS has been received, the respective investigation is carried out to determine whether or not the complaint, claim or appeal exists. If it does exist, it is determined which area is responsible for taking administrative or technical action and whether corrective or preventive action is required, in which case the action procedure must be applied.

Once the investigation has been generated, the response is evaluated in order to subsequently take the decision that resolves the complaint and its final communication to the subscriber, responsible party or interested party.

2.3 Name and identification of the document

The CPD for ECD will be called "Certification Practice Statement (CPD). The version changes according to the modifications on the same document.

LLEIDA.NET is a Registered Private Enterprise with the international organisation IANA (Internet Assigned Numbers Authority), with private code No 53589 under branch 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise). The above information can be consulted at the URL, by searching for the code 52376 https://www.iana.org/assignments/enterprise-numbers

DOCUMENT DATA:

Name of the document	Certification Practice Statement of LLEIDA S.A.S.
Description of the document	This document describes the operations and practices used by LLEIDA S.A.S. for the administration of its services as a Digital Certification Authority.
Version	2
OID	1.3.6.1.4.1.53589.1.2.1
Location	https://www.lleida.net/docs/en/colombia-declaracion.pdf

2.4 Legal framework

The execution, interpretation, modification or validity of this CPS and its corresponding annexes shall be governed by the provisions of the Colombian legislation in force.

In particular:

- Single Decree of the Trade, Industry and Tourism Sector - DURSCIT, 1074 of 2015. This compiles all the regulations governing the country's trade, industry and tourism sectors, including those related to the National Quality Subsystem, electronic signatures and digital signatures, and the accreditation of digital certification entities.
- Law 527 of 1999: regulating access to and use of data messages.
- Decree 019 of 2012, which abolishes the activity of authorisation of digital certification entities by the Superintendence of Industry and Commerce, and establishes the obligation to be accredited by the National Accreditation Body of Colombia - ONAC.
- Decree 620 of 2020: General guidelines on the use and operation of digital citizen services.
- Law 2106 of 2019: By which rules are issued to simplify, eliminate and reform unnecessary formalities, processes and procedures existing in the public administration.
- Law 1581 of 2012: Whereby general provisions are issued for the Protection of Personal Data.
- Decree 333 of 2014 (Regulation of certification bodies).
- Law 1898 of 2018. Authentication and Digital Certificates.

In addition, the practices of the trust services provided by Lleida SAS follow the following standards or the modifications made where appropriate:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.

2.4.1 Dispute Settlement Mechanisms

If for any reason a dispute arises between the Parties (subscriber/responsible party and LLEIDA.NET) on the occasion of:

i. The provision of digital certification services as described in this CPS.

ii. during the execution of the contracted services.

iii. For the interpretation of the contract, DPC and any other document delivered by LLEIDA.NET.

The party concerned shall notify the other party via certified email of the existence of such a dispute, with full and duly substantiated information of the dispute, so that within fifteen (15) working days of such notification, the Parties may seek to reach a direct settlement between them as a first instance.

At the end of this period the dispute(s) persists, the Parties shall be free to resort to the Colombian ordinary justice to enforce their rights or demands, which shall be subject to the regulations in force on the matter, the costs caused on the occasion of the summons shall be entirely at the expense of the losing Party.

2.5 Definitions and acronyms

The following terms are commonly used and required for the understanding of this CPD.

2.5.1 Definitions

The following terms are commonly used and required for the understanding of this CPD.

Digital Certification Entity (EDC): A legal entity, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, entitled by the Colombian government (National Accreditation Body in Colombia) to issue certificates in relation to the digital signatures of customers who acquire them, offer or facilitate the services of registration and time stamping of the transmission and reception of data messages, as well as perform other functions relating to communications based on digital signatures.

Open Certification Entity: is a Certification Entity that offers services typical of certification entities, such as:

a. Its use is not limited to the exchange of messages between the entity and the subscriber; or

b. It receives remuneration for these.

Closed certification authority: An entity that offers certification authority services only for the exchange of messages between the certification authority and the subscriber, without remuneration.

Certification Service Provider (CSP). Certification Service Provider (CSP): a natural or legal person that issues digital certificates and provides other services related to digital signatures.

The Certification Authority (CA). Certification Authority (CA): Certification Authority, root entity and public key infrastructure certification services provider.

The Registration Authority (RA). Registration Authority (RA): The entity in charge of certifying the validity of the information provided by the applicant for a digital certificate, by verifying its identity and registration.

Intermediate Authorities: Subordinate CSPs that, under the hierarchy of a root certificate, issue digital certificates to end users.

Certification Practice Statement (CPS). Certification Practice Statement (CPS): a statement by the certification body of the policies and procedures it applies to the provision of its services.

The Certification Policy (CP). This is a set of rules that define the characteristics of the different types of certificates and their use.

Digital certificate: a document signed electronically by a certification service provider that links signature verification data to a signatory and confirms the signatory's identity. This is the definition in Law 527/1999, which in this document is extended to cases where the linking of signature verification data is made to a computer component.

Time stamping: According to numeral 7 of Article 3° of Decree 333 of 2014, it is defined as: Message of data with a specific moment or period of time, which allows to establish with a proof that these data existed at a moment or period of time and that they did not undergo any modification from the moment the stamping was performed.

Time Stamping Authority (TSA). Time Stamping Authority (TSA): Certification body providing time stamping services.

Applicant: any natural or legal person requesting the issuance or renewal of a Digital Certificate.

Subscriber: person in whose name a certificate is issued.

Bona fide third party, relying third party, relying party: person or entity other than the subscriber or controller that decides to accept and rely on a digital certificate issued by the ECD.

Public Key Infrastructure (PKI). An acronym for "Public Key Infrastructure": a PKI is a combination of hardware and software, security policies and procedures that allows users of a basically insecure public network such as the Internet to exchange data messages in a secure manner using a pair of cryptographic keys (one private and one public) that are obtained and shared through a trusted authority.

Initiator: a person who, acting on his own account, or on whose behalf he has acted, sends or generates a data message.

Public Key and Private Key: the asymmetric cryptography on which PKI is based. It uses a pair of keys in which one key is encrypted with one of them and can only be decrypted with the other and vice versa. One of these keys is called public and is included in the digital certificate, while the other is called private and is known only to the subscriber or certificate holder.

Private key (Private key): A numeric value or values which, when used in conjunction with a known mathematical procedure, is used to generate the digital signature of a data message.

Public key (Public key): numerical value(s) that are used to verify that a digital signature was generated with the private key of the originator.

Personal Identification Number (PIN). Personal Identification Number: Sequence of characters that allow access to the digital certificate.

Repository: information system used to store and retrieve certificates and other related information.

Certificate Revocation List: (CRL). Certificate Revocation List: List where only revoked certificates that have not expired are listed.

Compromise of the private key: meaning theft, loss, destruction, disclosure of the private key that could jeopardise the use and use of the certificate by unauthorised third parties or the certification system.

Trust hierarchy: A set of Certification Authorities that maintain trust relationships whereby a higher-level CA guarantees the trustworthiness of one or more lower-level CAs.

Cryptographic Hardware Security Module: hardware module used to perform cryptographic functions and store keys in secure mode.

PKCS#12: Personal Information Exchange Syntax Standard. Defines a file format commonly used to store private keys with their public key certificate protected by symmetric key, currently not supported as a mechanism to store private keys for subscribers.

Online Certificate Status Protocol (OCSP). Online Certificate Status Protocol (OCSP): Protocol that allows the status of a digital certificate to be verified online.

Holder. Entity that requires the services provided by LLEIDA.NET and that agrees with the terms and conditions published on the https://www.lleida.net/docs/es/colombia-declaracion.pdf of the services as stated in this document.

ECD LLEIDA.NET: This is the Certification Authority of LLEIDA.NET, a provider of digital Certification Services.

AR/RA LLEIDA.NET: This is the LLEIDA.NET Registration Authority, the provider of the LLEIDA.NET registration service in the process of requesting, identifying and approving applicants for a digital certificate.

TSA LLEIDA.NET: Corresponds to the term used by ECD LLEIDA.NET, in the provision of its Time Stamping service, as Time Stamping Authority.

2.5.2 Acronyms

CA: Certification Authority

CA Sub: Subordinate Certification Authority

CP: Certificate Policy

CPD: Certificate Practice Statement (Certificate Practice Statement)

CRL: Certificate Revocation List CSP: Certification Service Provider

DNS: Domain Name System

FIPS: Federal Information Processing Standard

HTTP: HyperText Transfer Protocol (HTTP) is the protocol used in every transaction on the World Wide Web (WWW). HTTP defines the syntax and semantics used by the software elements of the web architecture (clients, servers, proxies) to communicate. It is a transaction-oriented protocol and follows the request-response scheme between a client and a server.

HTTPS: Hypertext Transfer Protocol Secure, better known by its acronym HTTPS, is a network protocol based on the HTTP protocol, intended for the secure transfer of hypertext data, i.e. it is the secure version of HTTP.

HSM: Hardware Security Module (HSM)

IEC: International Electrotechnical Commission

IETF: Internet Engineering Task Force (Internet Standardisation Organisation)

IP: Internet Protocol

ISO: International Organization for Standardization

LDAP: Lightweight Directory Access Protocol OCSP: Online Certificate Status Protocol.

OCSP: Online Certificate Status Protocol

OID: Object identifier (Unique Object Identifier)

PIN: Personal Identification Number

PUK: Personal Unlocking Key

PKCS: Public Key Cryptography Standards. PKI standards developed by RSA Laboratories and accepted internationally.

PKI: Public Key Infrastructure

PKIX: Public Key Infrastructure (X.509)

QSCD: Qualified (electronic) Signature Creation Device - Qualified (electronic) Signature Creation Device

RA: Registration Authority

RFC: Request For Comments (Standard issued by the IETF)

HR:Human Resources

ISMS:Information Security Management System

URL: Uniform Resource Locator

VA: Validation Authority

2.5.3 Standards and standardisation bodies

CEN: European Committee for Standardisation

CWA: CEN Workshop Agreement

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard

IETF: Internet Engineer Task Force

PKIX: IETF PKI Working Group PKCS: Public Key Cryptography Standards RFC: Request For Comments

PKCS: Public Key Cryptography Standards

RFC: Request For Comments

2.6 Participants

2.6.1 Digital Certification Authority (DCA or ECD)

It is that legal person, accredited in accordance with Law 527 of 1999 and Decree 333 of 2014, empowered by the Colombian government or the National Accreditation Body in Colombia to provide digital certification services in accordance with the provisions of Law 527 of 1999, Decree Law 0019 of 2012, Decree 333 of 2014, Decree 1471 of 2014 and the regulations that modify or complement them, is the origin of the digital certification hierarchy that allows it to provide services related to communications based on public key infrastructures.

LLEIDA.NET has as Digital Certification Body (ECD):

Name: LLEIDA SAS
Tax Identification Number: 900571038-3
Nature: Private (Public Limited Company)
Type of company SME
Address: Calle 81 # 11 - 55 Office 903
City / Country: Bogotá D.C., Colombia.
Telephone: +57 (1) 3819903
E-mail: co@lleida.net
Website: www.lleida.net/co

2.6.2 Registration Authority (RA)

It is the entity in charge of certifying the validity of the information provided by the applicant for a digital certification service, through the verification of the entity of the subscriber or person responsible for the digital certification services, in the RA deciding on the issuance or activation of the digital certification service.

Under this CPS, the figure of RA is part of the ECD itself and may act as a Subordinate of ECD LLEIDANET.

LLEIDANET has as registration authority RA:

Name: LLEIDA SAS
Tax Identification Number: 900571038-3
Nature: Private (Public Limited Company)
Type of company SME
Address: Calle 81 # 11 - 55 Office 903
City / Country: Bogotá D.C., Colombia.
Phone: +57 (1) 3819903
E-mail: co@lleida.net
Website: www.lleida.net/co

RA functions may be outsourced. In this case, LLEIDA.NET's RA will assess compliance with its policies by carrying out internal assessments to determine compliance with said third party.

The RA may outsource the verification and registration functions without any limit or restriction, always making it clear that the RA is ultimately responsible, provided that the integrity and authenticity of the transactions in the authorisation of requests for issuance, revocation, re-issuance (which is carried out through our PKI platform) is ensured. However, the legal responsibility towards the Supervisory Authority, subscribers, holders and relying third parties lies with the entity applying for accreditation of the Registry Entity. The third party must guarantee the security and protection of the RA's personal and confidential data, as well as the integrity and authenticity of transactions in the authorisation of requests for issuance, revocation, re-issuance, during the execution of outsourcing activities, it being clear that before the Supervisory Body the RA is responsible before third parties.

It should be noted that LLEIDA.NET provides the third party with the RA Platform for the creation of the application and the issuance of certificates, ensuring integrity throughout the process, accessing the platform with the operator's digital certificate.

2.6.2.1 Certificates managed by the Registration Authority

Below are the certificates that are managed by the Registration Authority of LLEIDA.NET

Name of the certificate	OID	OID QCP	QCP

Certification Policies Natural Person Certificates	1.3.6.1.4.1.53589.1.1.1		
Natural Person Software	1.3.6.1.4.1.53589.1.1.1.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Natural Person Hardware	1.3.6.1.4.1.53589.1.1.1.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Natural Person eSignaId	1.3.6.1.4.1.53589.1.1.1.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Natural Person Centralised UP	1.3.6.1.4.1.53589.1.1.1.3.2	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Natural Person Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.1.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Company Membership Certificates	1.3.6.1.4.1.53589.1.1.2		
Software Company Membership	1.3.6.1.4.1.53589.1.1.2.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Hardware Company Membership	1.3.6.1.4.1.53589.1.1.2.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
eSignaId Company Membership	1.3.6.1.4.1.53589.1.1.2.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Company Membership Centralised UP	1.3.6.1.4.1.53589.1.1.2.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Company membership Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.2.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Certificates Company Representation	1.3.6.1.4.1.53589.1.1.3		
Software Company Representation	1.3.6.1.4.1.53589.1.1.3.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Hardware Company Representation	1.3.6.1.4.1.53589.1.1.3.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
eSignaID Company Representation	1.3.6.1.4.1.53589.1.1.3.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)

Company Representation Centralised UP	1.3.6.1.4.1.53589.1.1.3.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Company representation Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.3.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Civil Service Certificates	1.3.6.1.4.1.53589.1.1.3.5		
Civil Service Software	1.3.6.1.4.1.53589.1.1.3.5.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Civil Service Hardware	1.3.6.1.4.1.53589.1.1.3.5.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Civil Service eSignaId	1.3.6.1.4.1.53589.1.1.3.5.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Civil Service Centralised UP	1.3.6.1.4.1.53589.1.1.3.5.4	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Civil Service Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.3.5.5	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Certificate of Juridical Status	1.3.6.1.4.1.53589.1.1.3.4	0.4.0.194112.1.1	
Legal Person Software	1.3.6.1.4.1.53589.1.1.3.4.1	0.4.0.194112.1.1	QCP-l-E-Stamp (LLEIDA SAS SUB CA CO 001)
Legal Entity Hardware	1.3.6.1.4.1.53589.1.1.3.4.2	0.4.0.194112.1.1	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Legal Entity Centralised UP	1.3.6.1.4.1.53589.1.1.3.4.4	0.4.0.194112.1.1	QCP-n-qscd (Lleida SAS SUB CA CO 001)

2.6.2.2 Description of the Certificates managed by the Registration Authority

INFORMATIVE NOTE: All software certificates are issued in the PKCS#12 format which is considered NOT ACCEPTABLE according to Annex G of the SPECIFIC CRITERIA FOR ACCREDITATION OF DIGITAL CERTIFICATION ENTITIES (CEA-3.0-07). These certificates are issued for those restricted domains that wish to accept them and are NOT ACCREDITABLE by ONAC.

Certificates issued on tokens and cryptographic cards may NOT be used on computers running Mac OS.

Each Certificate Policy is identified with a differentiated OID and in accordance with the hierarchy of OIDs defined for LLEIDA SAS. The following table describes the different Policies, the handling of which is described in the corresponding sections of this CPS:

Name	OID	Description
Natural Person		
Natural Person Software	1.3.6.1.4.1.53589.1.1.1.1.1	Certificate that allows a natural person to have a digital certificate issued on their computer and to use it with any application, entity and public administration that decides to use it in a restricted area. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with limited legal guarantees. LEGAL GUARANTEES Limited
Natural Person Hardware	1.3.6.1.4.1.53589.1.1.1.2.1	Certificate that allows a natural person to have a digital certificate issued in a qualified cryptographic device (token or cryptographic card), which gives greater security to the use and custody of the certificate, this device will need an external device that will allow it to work in the computer, with this you can access any entity and public administration, thus avoiding unnecessary travel and waiting. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and its implementing regulations.
Natural Person eSignaId	1.3.6.1.4.1.53589.1.1.1.3.1	Certificate that allows a natural person to have a qualified digital certificate issued on their mobile phone, for use from LLEIDA.NET eSigna applications, such as eSignaBox. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature. The eSignaID ( ) digital certificate of Natural Person will be issued on the mobile phone of the certificate subscriber,

		who will have exclusive use and access to the private keys of the certificate. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Natural Person Centralised UP	1.3.6.1.4.1.53589.1.1.1.3.2	Certificate that allows a natural person to have a qualified digital certificate of centralised signature with access to it by means of credentials (username and password) and a PIN known only to the subscriber. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Natural Person Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.1.3.3	Certificate that allows a natural person to have a qualified centrally signed digital certificate with access to it by means of a fingerprint and a PIN known only to the subscriber. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and its implementing regulations.
Belonging to Company		
Software Company Membership	1.3.6.1.4.1.53589.1.1.2.1.1	It is a certificate that digitally identifies a natural person and links them to an organisation or entity by informing the position they hold in it, whether they are an employee, associate, collaborator, client or supplier. Digital signature without powers of attorney. The certificate allows its holder to make digitally signed communications accrediting their membership of a specific organisation, but does not grant them any powers greater than those they have for

		the normal performance of their activity. It is not suitable for proxies or general representatives, as it does not provide information on the existence of powers of attorney. The digital certificate will be issued on the subscriber's computer, so it can be used with any application, entity and public administration that decides to use it in a restricted area. LEGAL GUARANTEES Limited
Hardware Company Membership	1.3.6.1.4.1.53589.1.1.2.2.1	It is a qualified certificate that digitally identifies a natural person and links them to an organisation or entity by informing them of their position in it, whether they are an employee, associate, collaborator, client or supplier. Digital signature without powers of attorney. The certificate allows its holder to make digitally signed communications accrediting their membership of a specific organisation, but does not grant them any powers greater than those they have for the normal performance of their activity. It is not suitable for proxies or general representatives, as it does not provide information on the existence of powers of attorney. The digital certificate will be issued in a qualified cryptographic device (token or cryptographic card), which gives greater security to the use and custody of the certificate, this device will need an external device that will allow it to run on the computer, so that it can be used with any application, entity and public administration, thus avoiding unnecessary travel and waiting. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and its implementing regulations.
eSignaId Company Membership	1.3.6.1.4.1.53589.1.1.2.3.1	It is a qualified certificate that digitally identifies a natural person and links them to an organisation or entity by informing them of their position in it, whether they are an employee, associate, collaborator, client or supplier. Digital signature without power of attorney

		The certificate allows its holder to make digitally signed communications accrediting their membership of a specific organisation, but does not grant them any powers greater than those they have for the normal performance of their activity. It is not suitable for proxies or general representatives, as it does not provide information on the existence of powers of attorney. The digital certificate will be issued on the certificate subscriber's smartphone and the subscriber will have exclusive use and access to the private keys of the certificate. More information on the eSigna ID application (available for iOS and Android) can be found at https://www.esignaid.com/. USABILITY eSignaID facilitates the identification and signature process through the use of the mobile phone, eliminating the complications of digital certificates. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and its implementing regulations.
Company Membership Centralised UP	1.3.6.1.4.1.53589.1.1.2.3.2	It is a qualified certificate that digitally identifies a natural person and links them to an organisation or entity by informing them of their position in it, whether they are an employee, associate, collaborator, client or supplier. Digital signature without powers of attorney. The certificate allows its holder to make digitally signed communications accrediting their membership of a specific organisation, but does not grant them any powers greater than those they have for the normal performance of their activity. It is not suitable for proxies or general representatives, as it does not provide information on the existence of powers of attorney. The digital certificate will be centrally signed with access to it by means of credentials (username and password) and a PIN known only to the subscriber. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of

		Law 527 of 1999 and the regulations that develop it.
Company membership Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.2.3.3	It is a qualified certificate that digitally identifies a natural person and links them to an organisation or entity by informing them of their position in it, whether they are an employee, associate, collaborator, client or supplier. Digital signature without powers of attorney. The certificate allows its holder to make digitally signed communications accrediting their membership of a specific organisation, but does not grant them any powers greater than those they have for the normal performance of their activity. It is not suitable for proxies or general representatives, as it does not provide information on the existence of powers of attorney. The digital certificate shall be centrally signed with access to it by means of a fingerprint and a PIN known only to the subscriber. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Company Representation		
Software Company Representation	1.3.6.1.4.1.53589.1.1.3.1.1	Certificate that allows a natural person to hold the status of legal representative with general powers of attorney of an organisation and to have a digital certificate issued to install it on their computer and to use it in any application or entity that decides to use it in a restricted area. LEGAL GUARANTEES Limited
Hardware Company Representation	1.3.6.1.4.1.53589.1.1.3.2.1	Qualified certificate that allows a legal person to hold the status of legal representative with general powers without limitations, of an organisation and to have a digital certificate issued in a qualified cryptographic device (token or cryptographic card) which gives greater security to the use and custody of the certificate, this device will need an external device that will allow it to operate in the computer. LEGAL GUARANTEES

		The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
eSignaID Company Representation	1.3.6.1.4.1.53589.1.1.3.3.1	Qualified certificate that allows a legal person to hold the status of legal representative with unlimited general powers of an organisation and have a digital certificate issued on their smartphone for use from LLEIDA.NET's eSigna applications, such as eSignaBox. The Legal Representative Legal Entity digital certificate (eSignaID) will be issued on the certificate subscriber's smartphone and the subscriber will have exclusive use and access to the private keys of the certificate. More information on the eSigna ID application (available for iOS and Android) can be found at More information on eSignaID. USABILITY eSignaID facilitates the identification and signature process through the use of the smartphone, eliminating the hassle of digital certificates. SECURITY eSignaID technology offers high security throughout the process, employing two-factor authentication mechanisms, protecting communications through SSL and encryption of information at the application and server level. LEGAL GUARANTEES The digital identity and the processes carried out with eSignaID comply with the provisions of Law 527 of 1999 and its implementing regulations.
Company Representation Centralised UP	1.3.6.1.4.1.53589.1.1.3.3.2	Qualified certificate that allows a legal person to hold the status of legal representative with unlimited general powers of attorney of an organisation and to have a centralised digital signature certificate. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Company representation Fingerprinting	1.3.6.1.4.1.53589.1.1.3.3.3	Qualified certificate that allows a legal person to hold the status of legal representative with unlimited general powers of attorney of an organisation and

		to have a centralised digital signature certificate. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Civil Service		
Civil Service Software	1.3.6.1.4.1.53589.1.1.3.5.1	Certificate that allows a natural person linked to the Public Administration to have a digital certificate issued on their computer and to use it with any application, entity and public administration that decides to use it in a restricted area. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees. LEGAL GUARANTEES Limited
Civil Service Hardware	1.3.6.1.4.1.53589.1.1.3.5.2	Certificate that allows a natural person linked to the Public Administration to have a digital certificate issued in a qualified cryptographic device (token or cryptographic card), which gives greater security to the use and custody of the certificate, this device will need an external device that will allow it to run on the computer, thus allowing access to any entity and public administration, avoiding unnecessary travel and waiting. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and its implementing regulations.
Civil Service eSignaId	1.3.6.1.4.1.53589.1.1.3.5.3	Certificate that allows a natural person linked to the Public Administration to have a qualified digital certificate issued on their mobile phone, for use from LLEIDA.NET's eSigna applications, such as eSignaBox. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature.

		The digital certificate of Función Pública eSignaID ( ) shall be issued on the mobile phone of the subscriber of the certificate and the subscriber shall have exclusive use and access to the private keys of the certificate. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Civil Service Centralised UP	1.3.6.1.4.1.53589.1.1.3.5.4	Certificate that allows a natural person linked to the Public Administration to have a qualified digital certificate of centralised signature with access to it by means of credentials (username and password) and a PIN that only the subscriber knows. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Civil Service Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.3.5.5	Certificate that allows a natural person linked to the Public Administration to have a qualified digital certificate of centralised signature with access to it by means of their fingerprint and a PIN known only to the subscriber. By means of this certificate you will be able to carry out authentication operations and digitally sign documents with full legal guarantees, it is the same, in terms of validity, as your handwritten signature. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and its implementing regulations.
Legal Entity		
Certificate of Legal Person Software	1.3.6.1.4.1.53589.1.1.3.4.1	This entity seal certificate allows a legal entity to identify itself telematically and to make electronic signatures in restricted and limited areas. Represents the entity to which the certificate has been issued, including its name, locality and tax identification number.

		LEGAL GUARANTEES Limited.
Certificate of Legal Entity Hardware	1.3.6.1.4.1.53589.1.1.3.4.2	This entity seal certificate allows a legal entity to identify itself telematically and to make electronic signatures without the need to incorporate the details of a representative. Unambiguously represents the entity to which the certificate has been issued, including its name, location and tax identification number. The seal certificate has a flexible configuration that allows for different uses: Electronic seals to guarantee, by means of electronic signature, the authenticity and integrity of the electronic documents to which they are linked. Authentication of IT components of an entity in their access to IT services or other technological infrastructures, with restricted access or client identification. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of Law 527 of 1999 and the regulations that develop it.
Centralised Legal Entity Certificate UP	1.3.6.1.4.1.53589.1.1.3.4.4	This entity seal certificate allows a legal entity to identify itself telematically and to make electronic signatures without the need to incorporate the details of a representative. Unambiguously represents the entity to which the certificate has been issued, including its name, location and tax identification number. The seal certificate has a flexible configuration that allows for different uses: Electronic seals to guarantee, by means of electronic signature, the authenticity and integrity of the electronic documents to which they are linked. Authentication of IT components of an entity in their access to IT services or other technological infrastructures, with restricted access or client identification. LEGAL GUARANTEES The digital identity and the processes carried out comply with the provisions of

		Law 527 of 1999 and the regulations that develop it.

2.6.3 Subscriber

Subscriber is the natural or legal person to whom the digital certification services are issued or activated and therefore acts as the subscriber or person responsible for the same in reliance thereon, with knowledge and full acceptance of the rights and duties established and published in this CPS.

The figure of Subscriber will be different depending on the services provided by Lleida.net as established in the Certification Policy.

In the case of certificates, it is the person responsible for the use of the private key, who is exclusively bound to a digitally signed electronic document using his private key.

In the event that the holder of the digital certificate is a natural person, he/she shall be the subscriber.

In the event that a legal entity is the holder of a digital certificate, the subscriber responsibility shall lie with the legal representative designated by this entity. If the certificate is designated for use by an automated agent, the ownership of the certificate and of the digital signatures generated from said certificate shall correspond to the legal entity. The attribution of subscriber responsibility, for such purposes, corresponds to the same legal entity.

2.6.4 Bona fide third party

Bona fide third parties are all those natural or legal persons who decide to accept and trust the digital certification services issued by the ECD to a subscriber or responsible party. The bona fide third party, in turn, may or may not be a subscriber.

2.6.5 Other participants

2.6.5.1 Time stamping authority

LLEIDA.NET in its role as Time Stamping Authority, is the private legal entity that provides indistinct registration and time stamping services in the generation, transmission and reception of data messages.

2.6.5.2 DIGITAL CERTIFICATION SERVICE PROVIDER

Certification service providers are third parties that provide their infrastructure or technological services to the Digital Certification Authority. LLEIDA.NET, when the certification body so requires and guarantee the continuity of the service to the holders for as long as the digital certification services have been contracted.

2.6.5.3 PROVIDER OF CENTRALISED SIGNATURE SERVICES AND QUALIFIED SIGNATURE AND STAMP VALIDATION SERVICE (LLEIDA.NET)

LLEIDA.NET acts as the provider of the centralised signature application service (SSASP) and the signature and stamp validation service.

2.6.5.4 SECURITY COMMITTEE

The security committee is an internal body of the Certification Body LLEIDA.NET which has, among other functions, the approval of the CPS as the initial document, as well as authorising the required changes or modifications to the approved CPS and authorising its publication. The Security Committee is responsible for integrating the CPS into the CPS of third party certification service providers.

2.7 Policy on the Use of Certification Services

2.7.1 Registeres e-mail

The Registered Electronic Mail service guarantees the reception of the message, ensuring at all times the characteristics of traceability and integrity. To this end, the service guarantees the receipt of messages by means of the evidence document, documents that are time stamped.

Registered e-mail can be used by a natural or legal person regardless of the e-mail client used. The use of registered e-mail does not depend on a device on the part of the recipient of the e-mail message, making it possible to obtain guarantees of receipt different from those offered by standard e-mail. The platform meets the need to provide traceability and guarantee the date and time of generation of the acknowledgement of receipt, in addition to integrating essential information within the documentary evidence that enables full equivalence to physical postal mail.

2.7.2 Registered SMS

The Registered SMS service allows you to guarantee the reception of the text message, always ensuring the characteristics of traceability and integrity. To this end, the service allows you to guarantee the receipt of messages by means of the evidence document, documents that are time stamped.

The Registered SMS can be used by a natural or legal person. By means of a platform that is made available to the subscriber, the message is sent as Lleida.net is a telecommunications operator and the information is obtained on the delivery status of the message. The expert evidence is generated whether it has delivery confirmation or not, indicating this characteristic in addition to the sender/subscriber details of the message, the recipient's mobile phone and the content of the message.

2.7.3 Click&Sign

Service that allows the composition and use of a signature process for PDF documents by the Lleida.net user based on the signature methods provided, such as acceptance by pressing a button in a web environment, introduction of an OTP, biometric handwritten signature or signature with an electronic certificate in the cloud.

The service is flexible so that the sender can configure the branding, the type of signature, the communications to the sender, the signatory or others, the request for document uploading to the signatory, the sending of signature reminders and the reception of signature status notification events, among others.

The issuer can make signature requests defining the recipients, the PDF documents to be signed, aspects such as the number of signatories, whether a signature is required in a specific order and the number of signatories required for the signature to be considered effective. In all cases, the service will generate a signed evidence with a time stamp that will compile all the traceability of registered communications carried out and actions performed by the signatory, thus accrediting their signature. If the process expires, an evidence document is issued to this effect.

In the case of biometric signature, the document with the embedded biometric signature will be additionally generated digitally signed and time stamped.

In the case of signing with an electronic certificate in the cloud, the document with the digital signature made in the cloud will also be generated.

2.7.4 Openum

Service that allows the composition and use of a PDF document notification process by the Lleida.net user based on the notification methods provided, such as sending notification by certified e-mail or not, sending notification by certified SMS or not, and viewing PDF documents.

The service is flexible so that the sender can configure the branding, the type of notification, the communications to the sender, the signatory or others, the request for document upload to the recipient, the sending of display reminders and the receipt of delivery status notification events, among others.

The sender may make notification requests by defining the recipients, the PDF documents to be notified, aspects such as the number of recipients, whether notification is required in a particular order and how many views are required for the notification to be considered effective.

In all cases, the service will generate signed evidence with a time stamp that will compile all the traceability of certified communications made and actions carried out by the addressee, thus accrediting its notification. If the process expires, an evidence document is issued to that effect.

The service is offered through a web-based user tool and API for sending, consulting and downloading documents.

2.7.5 eKYC

It consists of a non-face-to-face identification procedure by means of a videoconference that can be assisted or automatic, which includes the validation process of identification documents.

The service records the videoconference using WebRTC technology and captures images of the front and back of the identity document, as well as a selfie. After the capture, a series of identity validation parameters are obtained from the validation of the images, including facial biometrics. After the analysis, the system performs a validation of the parameters obtained, being able to define different logics according to the business needs to classify the identification process as positive or negative. The service issues digitally signed evidence with a time stamp that includes the images, a hash of the video, the validation data obtained, the result of the validation logic and the geolocation if the user allowed its activation.

2.7.6 Certificates

2.7.6.1 Certificate profiles

Lleida SAS issues the following certificate profiles with the characteristics and legal guarantees set out in the corresponding service policy:

- Issuance of digital certificates for legal entities on local or centralised devices
- Issuance of digital certificates for natural persons on local or centralised devices
- Issuance of digital certificates for public officials on local or centralised devices
- Issuance of digital certificates for entity representative on local or centralised devices
- Issuance of digital certificates for entity member on local or centralised devices

2.7.6.2 Signature in the Cloud

The SSASC service forms part of the services operated by LLEIDA S.A.S. and allows the centralised electronic signature service to be provided to signatories who have an electronic certificate defined for centralised signature in their corresponding Declaration of Practices Centralised Signature Service.

The service allows the creation of signatures through centralised signature systems, where LLEIDA S.A.S. manages the signature creation device on behalf of the signatory, enabling it to generate qualified electronic signatures, ensuring the signatory's exclusive control over its signature keys, either through authentication mechanisms plus OTP (user and password and OTP PIN), fingerprint or through the use of the eSignaID mobile APP, in accordance with the ETSI TS 119 431-1 technical specification.

2.7.7 Certificate validation

The LLEIDA S.A.S. Validation Platform for electronic signatures and seals responds to the Qualified Service for the validation of electronic signatures and seals, certified under the legal framework, which allows the corresponding evidence of validation of qualified certificates, electronic signatures and seals to be generated.

The Qualified Electronic Signature Validation Service generates evidence, taking into account the norms and standards established by current legal regulations. Checks are performed on the certificate's qualification status at the time, day and hour of issue. If an electronic Time Stamp exists, it is also checked. Likewise, the status of the certificate is checked at the time of signature. The corresponding evidence is generated for all processes.

It allows the consumer to be fully aware of the validity, force and regulatory compliance of the signature submitted for validation and allows him/her to establish internal policies to protect him/herself against documents or files signed by customers, suppliers or workers that do not comply with the provisions of the regulations.

2.7.8 Time Stamping

LLEIDA.NET's time stamping service allows the generation of time stamps.

Timestamp: A data set representing the summary of a stamped document added to a record of the time when the stamp was issued. This summary is a unique characteristic of the document, so that if the document is modified this time stamp becomes invalid.
The time stamp includes:

The digital signature of the time-stamping entity

-Unique electronic document identifier (HASH or summary)

-Date and time collected from a reliable time source

The LLEIDA.NET Time Stamping Policy has a unique identifier:

1.3.6.1.4.1.53589.1.1.5.3

2.8 Policy administration

2.8.1 Organisation administering the document

LLEIDA SAS, with registered office at Calle 81 # 11 - 55 Oficina 903 in Bogotá D.C. (Colombia), is the Certification Authority providing the services certified under this Certification Practice Statement.

2.8.2 Contact

Name of the ECD	LLEIDA SAS
Address	Calle 81 # 11 - 55 Office 903 Bogotá D.C.
Email address	info@lleida.net
Telephone	(+57) 1 381 9903

2.8.3 CPS compliance officers

The LLEIDA.NET Security Committee has, within its competencies, the capacity to specify, review and approve the review and maintenance procedures, both for this Certification Practices Statement, as well as for the Particular Certification Practices and the corresponding Certification Policy.

2.8.4 Approval procedure for certificate policies

LLEIDA.NET's Policy Approval Body is the Security Committee. It approves the final changes made to this document once it has determined that they comply with the established requirements. Once the changes have been approved, they will be published on the LLEIDANET website https://www.lleida.net/co.

The ECD Supervisor is responsible for ensuring that the provision of LLEIDANET services complies with the provisions of these Policies and Statement of Practice and for ensuring the effective implementation of the planned controls. He/she is also responsible for the management, supervision and control of the provision of LLEIDANET services, the operation of the service and the correct application of the provisions of this document.

The ECD Supervisor is also responsible for analysing the reports of the total or partial audits of LLEIDA.NET and its services, as well as for establishing and supervising, if necessary, the corrective actions to be taken.

The ECD Supervisor will be appointed and dismissed by the LLEIDA.NET management, by means of an express resolution which must be recorded in writing.

3 PUBLICATION AND REPOSITORY RESPONSIBILITIES

3.1 Repositories

The ECD provides revocation information for Subordinate Certificates and Subscriber Certificates made available in accordance with this Certification Practice Statement.

The certification policies and the certification practice statement will be available at the URL

- https://www.lleida.net/co/politicas-y-practicas

Consultation services are designed to ensure 24/7 availability.

Services Root Certificate

https://certs.esigna.es/root/ca_root_lleidasas.crt

Subordinate Certificate

https://certs.esigna.es/ca/lleidasas_pki_001.crt

List of Revoked Certificates (CRL)

https://crl1.esigna.es/sub/lleidasas_pki_001.crl

https://crl.esigna.es/sub/lleidasas_pki_001.crl

Certificate Validation

http://ocsp2.esigna.es

3.2 Publication of certification information

The ECD publicly discloses its Certificate Policy and/or Certification Practices Statement through an appropriate and easily accessible online medium that is available 24 hours a day, 7 days a week. A ECD shall publicly disclose its ECD business practices to the extent required by the selected audit scheme.

The URL where the policy information and Certification Practice Statement is available is:

https://www.lleida.net/es/politicas-y-practicas

It also contains the models and minutes of the contracts that they will use with the users.

Information on the Terms and Conditions for the provision of the various services will also be available at https://www.lleida.net.

Information on the status of valid digital certificates is available for consultation via OCSP protocol.

The disclosure includes all material required by RFC 2527 or RFC 3647 and is structured in accordance with RFC 2527 or RFC 3647.

3.3 Time or frequency of publication

LLEIDANET undertakes to make the Certification Policies and its Certification Practices Statement publicly available on its website as soon as they are approved by the Security Committee, when updates are made as a result of technical or legal changes.

LLEIDANET undertakes to develop, implement, enforce and update its Certification Policies and Certification Practices Statement on a biennial basis, as one of the elements associated with the biennial audit. The update interval will be shorter when technical or legal changes occur that make an update necessary.

Audits of the ECD for the issuance of digital certification services shall be annual.

Root Certificate

The root certificate shall be published and remain on the Digital Certification Authority's website for as long as digital certification services are being provided.

Subordinate Certificate

The certificate of the SubCA will be published and will remain on the website of the Digital Certification Authority for as long as digital certification services are being provided.

List of Revoked Certificates (CRL)

The Digital Certification Authority shall publish the list of revoked certificates on the website, in the events and with the frequency defined in the Frequency of issuance of CRLs.

Certificate Validation

The Digital Certification Authority will publish the certificates issued in a repository in X.509 V3 format, which can be consulted at the following address: http://ocsp2.esigna.es

3.4 Controlling access to repositories

Information regarding the status of digital certification services is available in read-only mode to relying parties.

LLEIDANET has implemented security controls to ensure that such access does not compromise the operation of the service. The function of these controls is to prevent unauthorised access, for example, to modify or delete data associated with the service, massive requests.

4 IDENTIFICATION AND AUTHENTICATION

4.1 Applicant

Any natural or legal person, legally authorised and duly identified, may apply for Lleida.net certification services.

Any person who requires the provision of the certified e-mail service may request this service via the Lleida.net website or by e-mail or telephone.

4.1.1 Types of names

The guidance document that LLEIDA.NET uses for the unique identification of issued certificate holders is defined in the Distinguished Name (DN) structure of the ISO/IEC 9594 (X.500) standard.

Certificates issued by LLEIDA.NET contain the X.500 distinguished name (DN) of the issuer and recipient of the certificate in the issuer name and subject name fields respectively.

4.1.1.1 LLEIDA.NET Root Certificate

The DN of the issuer name of the root certificate has the following fixed fields and values:

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

The following fields are included in the DN of the 'subject name':

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

Serial number = 34376792308506

Fingerprint = 4ba80d75903497f45d32efd25f184b362f1dd0

SHA-256 = EB2F7A6E156C096BB4D66B79AE70676E22456FA3073215AA16A0314F086040DE

4.1.1.2 Subordinated Debt Certificates

The DN of the issuer name of the certificates of the LLEIDA.NET. subordinates has the following characteristics:

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

The following fields are included in the DN of the 'subject name':

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

Serial number = 69782574365786

Fingerprint = d73c5ac77e345b2bea98da7c31b283e83e2b13a7

SHA-256 = C2F9D17FB87281FA9655A8E9AAEF4AC09BAA8F7597BEFD94ACE0F90C33B85C0C

4.1.1.3 Holder Certificates

The DN of the issuer name of the LLEIDA.NET. holder certificates has the following general characteristics:

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

The description and fields in the DN of the subject name, for each type of certificate covered by this CPS, are detailed in document DOC-220304-2242015- Certificate Profiles.pdf.

4.1.1.4 Meanings of Names

All Distinguished Names are meaningful, and the identification of the attributes associated with the subscriber must be in a human readable form. See 8.1.4 Name Format and Certification Policy document.

4.1.1.5 Anonymity or pseudonyms of subscribers

LLEIDA.NET. will use the pseudonym in the CN attribute of the Subject/Signatory's name, keeping the real identity of the Subject/Signatory confidential. The calculation of the pseudonym in those certificates where it is permitted is carried out in such a way that the real certificate holder is univocally identified.

4.1.1.6 Rules used to interpret various name formats

LLEIDA.NET uses for the unique identification of issued certificate holders is defined in the Distinguished Name (DN) structure of the ISO/IEC 9594 standard.

4.1.1.7 Uniqueness of names

Within the same EDC, a Subject/Signatory name that has already been occupied cannot be re-assigned to a different Subject/Signatory, this is achieved by incorporating the unique fiscal identifier into the name string that distinguishes the certificate holder.

Under this CPS a natural person Signatory can request more than one certificate as long as the combination of the following values in the request is different:

- NIT
- Identification document
- Certificate type: Policy identifier.
- A different certificate can also be considered when the position, title or department attribute in the certificate holder field is different.

4.1.1.8 Recognition, authentication and function of Trademarks and other distinctive signs

LLEIDA.NET makes no commitment to issue certificates regarding the use of trademarks and other distinctive signs.

LLEIDA.NET deliberately does not permit the use of a distinctive sign on the Subject/Signatory that does not hold rights of use.

However, LLEIDA.NET is not obliged to seek evidence of rights to use trademarks or other distinctive signs prior to the issuance of certificates, so it may refuse to generate or request the revocation of any certificate involved in a dispute.

4.1.1.9 Name dispute resolution procedure

LLEIDA.NET has no responsibility in the case of name dispute resolution. In any case, names will be assigned based on their order of entry. LLEIDA.NET does not arbitrate this type of dispute, which must be resolved directly by the parties.

4.2 Initial identity validation

The applicant's identification functions are carried out by Lleida.net's RA, who acts by order of the Commercial Department, which is the one who makes the request.

The RA will examine the documentation required for service activation and checks whether the information provided is valid and complies with the requirements defined for each policy of the services the customer intends to use.

4.2.1 Method of proving possession of the private key

To guarantee the issuance, possession and control of the private key by the subscriber, it is directly generated by the subscriber, using a secure cryptographic device "Hardware Security Module (HSM)", secure key generation and transmitted through a secure channel; or by means of a protected file using the PKCS#12 standard.

No storage services of originals, copies or back-ups of the subscriber's digital signature private key are performed in the RA or in the ECD.

4.2.2 Authentication of an organisation's identity (legal entity)

The RA should request the necessary documentation or information to ensure that a name or mark belongs to the applicant or principal of a digital certificate.

In the case of validation of legal persons, it shall not be possible to re-assign a holder name that has already been assigned to a different holder[1] .

The legal representative is accredited by proving the existence of the legal entity and its validity by means of public instruments or the respective legal norm. The identity of the legal entity must be verified:

In person:

- In the case of companies domiciled in Colombia, the existence and validity of the legal entity must be accredited with the certificate[2] or electronic consultation of validity issued by the Public Registers, the verification may also be carried out by means of consultation in the public register in which the incorporation and power of attorney documents are registered, using the telematic means provided by the aforementioned public registers.
- In the case of companies incorporated abroad, proof of their existence and validity shall be provided by means of a certificate[3] of the company's validity or other equivalent instrument or online consultation issued by the competent authority in their country of origin.

Telematically:

- The accreditation of the legal representative may be carried out telematically by means of video identification or biometric facial verification systems. This videoconference or the video identification or biometric facial verification process will be recorded and stored for later verification if necessary.
- The accreditation of the legal representative will be verified with the application of the public instruments indicated for when it is carried out in person.

When an individual applies for the issuance of a certificate serving to accredit the exercise of a particular office, evidence of the office, including the power to act on behalf of the legal person in which the office is held, is requested by means of a respective legal document or consultation of the respective database.

4.2.3 Authentication of the identity of the natural person making the application

After the application, the identity of the applicants must be validated in person, and they can be validated in any of the following ways:

In person:

[1] It is not for the RE to resolve any dispute concerning the ownership of names of natural or legal persons, domain names, trademarks or trade names.

[2] The validity of the certificate submitted must not exceed 30 days.

[3] The validity of the certificate must not exceed 30 days.

Proof of identity is provided by identity card, citizenship card, passport, aliens identity card or other legally recognised means. The appearance may be dispensed with if your signature on the application for the issue of a recognised certificate has been authenticated in the presence of a notary.

Telematically:

- Alternatively, the Applicant may choose to appear before a Notary Public and submit the request for the issuance of the certificate with his signature authenticated in the presence of a Notary Public.
- By means of another qualified certificate issued by the EDC of LLEIDA SAS or by another EDC, for which the physical personation or a notified electronic means of identification has been used, for the identification of the Applicant, provided that it is recorded to the Provider that the personation took place less than five years ago.
- Using other nationally recognised identification methods that provide equivalent security in terms of reliability to physical presence. The equivalent security shall be confirmed by a conformity assessment body.
- The accreditation of the applicant may be carried out telematically by means of video identification or biometric facial verification systems. This videoconference or the video identification or biometric facial verification process will be recorded and stored for later verification if necessary.
- The applicant's accreditation will be verified with the documents indicated for when it is done in person.

LLEIDA.NET has a Video Identification method based on the video-conference procedure and recognised in other European Union countries for the issuing of qualified certificates.

Brief description of the video signature:

- Requires Applicants to be equipped with a device with internet access (PC, tablet, smartphone, etc.), a camera and a sound system.

- The Operator sends the applicant a link for the applicant to agree to have his image recorded during the session and to indicate a unique operation code that uniquely links the certificate request he is making.

- The Operator shall proceed to the validation of the Applicant's proof of life and facial recognition against the Identity Card.

- The entire process is recorded so that it can be audited.

- Log data, i.e. audio and video files and structured metadata in electronic format, are stored in a protected form and in accordance with the European standard on personal data protection.

This video-signature identification method may be used to issue electronic certificates.

The collection and validation of the holder will be performed by the same person, with RA agent profile, who will subsequently issue the certificate.

4.2.4 Unverified subscriber information

Under no circumstances will LLEIDA.NET omit the verification work that leads to the identification of the Data Subject, which translates into the request to show the aforementioned documents for organisations and natural persons.

4.2.5 Authority validation

Type of certificate	Required Documentation
Natural Person	Colombian Nationality: • Identity Card. • Citizenship certificate Foreigners: • Passport • Aliens identity card For foreign identity documents, a Hague apostille will be required and a sworn translation may be requested if necessary. In addition, proof of address shall include either the RUT or a document issued by a third party verifying the address.
Entity Representation	The same as for validating the identity of the natural person plus: Photocopy of the document establishing their appointment as legal representative with an issue date of no more than thirty (30) days: - Chamber of Commerce (Private companies registered in RUES) - Certificate of appointment with the Colombian Financial Superintendency (supervised financial institutions). - Public Deed (Joint Venture and Consortia)
Entity Membership	The same as for validating the identity of the natural person plus: * Applicant's employment certificate with an issue date of no more than thirty (30) days (must be attached on company letterhead digitally signed by the legal representative or by the human resources area). * Document of Existence and Legal Representation of the Company, valid for no more than thirty (30) days.
Civil Service	The same as for validating the identity of the natural person plus: Photocopy of the document of appointment and acceptance of the position or certificate of the validity of the appointment and exercise of the position (these documents must show the dates of validity of the appointment and the number of the act of possession).
Legal Entity	Authorisation digitally signed by a legal representative or general proxy of the entity, with a digital certificate of legal representative or proxy issued by a trusted EDC or LLEIDA.NET. * Document of Existence and Legal Representation of the Company, valid for no more than thirty (30) days. Photocopy of the document establishing their appointment as legal representative with an issue date of no more than thirty (30) days:

4.2.6 Criteria for Interoperability

LLEIDA.NET may provide services that allow another ECD to operate within, or interoperate with, its PKI. Such interoperation may include cross certification, unilateral certification or other forms of operation. LLEIDA.NET reserves the right to provide interoperation services and interoperate with other ECDs; the terms and criteria for which are to be contractually established.

4.3 Identification and validation of renewal applications

Most of Lleida.net's digital certification services are automatically renewed, so if the user does not wish to use the service, he/she must inform the RA.

In the case of the certificate service, a renewal is required according to the following scenarios:

4.3.1 Identification and authentication in routine refurbishment tasks

The Digital Certification Authority carries out the authentication process of the applicant in all events, including renewals, and issues digital certificates on this basis.

The authentication procedures are described in section 4.2 Initial identity validation of this document.

4.3.2 Identification and authentication of the renewal request after revocation

Since a revocation implies the issuance of a new certificate, the Digital Certification Authority carries out a new authentication process of the applicant.

The authentication procedures are described in section 4.2 Initial identity validation of this document.

4.4 Identification and authentication for the request cancellation

The user may voluntarily request cancellation of the service at any time, but he/she is obliged to request cancellation of the service in the following situations:

a) Due to loss or disablement of credentials (username and password)
b) The credentials have been exposed or are at risk of misuse.
c) Changes in the circumstances under which Lleida.net authorised the service.

If the responsible party does not request the cancellation of the service in the event of the above situations, he shall be liable for any loss or damage incurred by third parties in good faith without fault who relied on the service.

In addition, it should be noted that revocation of a certificate can be requested and requires authentication according to the following criteria:

- Subscribers must present to the RA their identity card, citizenship card, passport, aliens identity card or other legally accepted means.
- The representative assigned by the legal entity must present documents accrediting said representation and the will of said legal entity, which must be accredited with the certificate[4] or electronic consultation of validity issued by the Public Registries, the aforementioned verification may also be carried out by means of consultation in the public registry in which the incorporation and power of attorney documents are registered, and may use the telematic means provided by the aforementioned public registries.
- Third parties (other than the ECD, the subscriber and the certificate holder) must submit to the RA reliable evidence of the misuse of the certificate in accordance with the applicable law, together with the respective court order.

The user acknowledges and accepts that Lleida.net services must be cancelled when the user knows or has indications or confirmation of the occurrence of any of the following circumstances:

a) At the request of the user or a third party acting on behalf of the user.

b) Due to a change of user.

c) Due to the death of the user.

d) By liquidation in the case of legal persons (entity) that acquired the service.

e) For confirmation or evidence that any information is false.

(f) on cessation of the activities of the certification body.

(g) By order of a court or competent administrative body.

(h) For compromise of security in any way, manner, situation or circumstance.

i) Due to the supervening incapacity of the person or entity responsible.

(j) Due to the occurrence of new facts that cause the original data not to correspond to reality.

(k) For the application of the terms and conditions document in accordance with the grounds set out in the contract.

l) For any cause that reasonably leads to believe that the service used with a digital certificate has been compromised to such an extent that the trustworthiness of the service is in doubt.

m) For improper handling by the person responsible for the service.

(n) for breach by the user or the legal entity it represents or to which it is bound by the terms and conditions document.

o) Knowledge of events that modify the initial status of the data provided, among others: termination of the Legal Representation, termination of the employment relationship, liquidation or extinction of the legal status, cessation of the public function or change to a different one.

p) At any time when there is evidence of false information provided by the applicant, subscriber or person responsible.

q) For failure on the part of Lleida SAS, the Subscriber or the person responsible for the obligations established in the Policy.

[4] The validity of the certificate submitted must not exceed 30 days.

r) Failure to pay the amounts for certification services agreed between the applicant and Lleida SAS.

However, for the above reasons, Lleida SAS may also cancel any of the services when, in its opinion, the credibility, reliability, commercial value, good name of the ECD, legal or moral suitability of the entire certification system may be put at risk.

5 LIFECYCLE OPERATIONAL REQUIREMENTS OF DIGITAL CERTIFICATION SERVICES

This Certification Practice Statement governs common operational requirements for digital certification services.

The Certification Policies of the different types of certificates may contain specificities regarding some aspect of their lifecycle.

5.1 Request from service

The application for services can be made by several methods, namely:

Telephone: +57 1 3819903

E-mail: info@lleida.net

Web forms available at www.lleida.net/co

The following service modalities are available to request the issuance of certificates:

- In person at the LLEIDA.NET RA facilities.
- In person at the customer's premises, or a location assigned by the customer in the presence of an RA representative.
- The appearance may be dispensed with if his signature on the application for the issue of a qualified certificate has been notarised in the presence of a notary.
- Telematically by means of video identification or biometric facial verification systems. This videoconference or the video identification or biometric facial verification process will be recorded and stored for later verification if necessary.

5.2 Who can submit an application for a certificate

A certification service can be requested by persons who:

- do so in their own name and on their own behalf
- Representatives of entities with or without legal personality, duly accredited

In particular for applications for the issuing of certificates:

In the case of natural persons, the application must be made by the same person who intends to hold the certificate or by a representative with express powers for this purpose granted by means of a power of attorney. In this case, the certificate holder shall be the principal and the authorised representative shall be the subscriber. The scope of use of the digital certificate in this case shall be circumscribed and limited to the powers expressly conferred in the power of attorney.

In the case of legal persons, attribute certificates may be requested for use by officials and specific personnel, including the legal representative. In this case, the legal entity is considered to be the applicant certificate holder and these natural persons are considered to be the applicant subscribers.

In the event that the certificate is intended for use by an automated agent, the application must be made by a representative appointed by the legal entity that owns the device. In this case, the ownership of the certificate and of the digital signatures generated from said certificate shall correspond to the legal person. The attribution of responsibility for such purposes corresponds to the legal representative, who on behalf of the legal person applies for the digital certificate.

5.3 Registration process and responsibilities

The RA receives the application information and forwards it to the Commercial Department, which contacts the subscriber and collects the identification documentation.

LLEIDANET, through its Sales Department, will provide information on the documentation required for identification and authentication, which can be done by remote identification mechanisms, normally by e-mail.

The documentation to be provided must be up to date and valid. Documents sent in digital format must be legible. If you opt for face-to-face verification of identity, the documents to be provided must be originals.

The tasks of identification and validation of information for the service and validation and approval of applications for issuance and revocation shall be carried out by the Registry Offices (RA) or telematically by means of video identification or biometric facial verification systems.

LLEIDA.NET's own registry offices or those of the user entities with which it has signed the corresponding legal instrument must assume the following obligations:

- Validate the identity and other personal details of the applicant, subscriber and or information relevant to the purpose of activating the services.
- Maintain all information and documentation relating to certificates, and manage their issue and revocation.
- Notify LLEIDA.NET of requests for revocation of services with due diligence and in a prompt and reliable manner.
- Allow LLEIDA.NET access to its procedural files and audit trails to perform its functions and maintain the necessary information.
- Inform LLEIDA.NET of requests for issue, revocation and any other aspect related to the services provided by LLEIDANET.
- Validate, with due diligence, the circumstances of revocation that may affect the validity of the service.

- Comply with the procedures established by LLEIDA.NET and with current legislation in this area, in its management operations related to the activation and revocation of services.

5.4 Certificate application procedure

Once a request for one or more services has taken place, the RA operator through access to the management platform verifies that the information provided is correct.

The LLEIDA.NET Registration Authority can issue the following certificates:

- Certificate of Natural Person
- Company Membership Certificate
- Company Representation Certificate
- Civil Service Certificate
- Certificate of Legal Entity.

For the issuing of certificates in person:

- The requirements are informed in person or sent by post to the Holder according to the type of certificate requested.
- Payment for the service or document evidencing the same is verified.
- On-site verification is carried out
- Accessing the Platform and selecting the type of certificate to be issued.
- If the cryptographic module is not part of the service, it is evaluated for compatibility with the Registry Platform[5] and that it is FIPS 140-2 level 3 or Common Criteria EAL 4+ certified[6] .
- Applications are made on the Registration Platform, attaching evidence of information.
- A contract for the issuance of the certificate is signed.
- Certificate is generated in PKI.
- It is inserted into the cryptographic module where the keys are generated.
- Activation and revocation key is received via declared e-mail.

For remote certificate issuance:

- Requirements are sent by mail to the Holder according to the type of certificate requested, indicating the legalisation of on-site verification and legalisation of the contract.
- The payment of the service and the sending of documents that support the requirements for issuance are verified.
- Accessing the Platform and selecting the type of certificate to be issued.

[5] The Registry platform only recognises modules with FIPS 140-2 level 3 minimum or Common Criterial EAL 4+, otherwise the process is stopped and the registrant is informed.

[6] If the administration of the cryptographic module is carried out by the Registrant, the responsibility lies with the Registrant.

- If the cryptographic module is not part of the service, it is evaluated for compatibility with the Registry Platform[7] and that it is FIPS 140-2 level 3 or Common Criteria EAL 4+ certified[8] .
- Applications are made on the Registration Platform, attaching evidence of information.
- A contract for the issuance of the certificate is signed.
- Certificate is generated in PKI.
- It is inserted into the cryptographic module where the keys are generated.
- Activation and revocation key is received via declared e-mail.
- Digital certificate is sent by secure transport or Courier if part of the service.

5.4.1 Performing identification and authentication functions

It is the responsibility of the RA to correctly carry out the identification of the subscriber. This process must be carried out prior to activation of the service.

In all cases, users should consult the specific documentation of each service for details on each of them. This is in accordance with section **¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**

5.4.2 Approval or rejection of certificate applications

Once the service(s) has been requested, the RA shall verify the information provided by the applicant, including validation of the subscriber's identity and, where applicable, the sufficiency of powers of attorney.

If the information is not correct, the RA will deny the request and contact the applicant to explain the reason. If the information is correct, the service activation process will continue.

Likewise, LLEIDA.NET reserves the right not to issue certificates even though the identification of the applicant and/or the information supplied by the applicant has been fully authenticated, when the issuing of a particular certificate for reasons of legal order and/or commercial convenience, good name or reputation of LLEIDA.NET ECD could jeopardise the digital certification system.

In case an application is approved by the RA, the following will take place:

> The ECD shall be notified of its approval for certificate issuance. To this end, the necessary security mechanisms must be implemented to establish secure communication between the ECD and the RA during the certificate issuance and key pair generation process.

[7] The Registry platform only recognises modules with FIPS 140-2 level 3 minimum or Common Criterial EAL 4+, otherwise the process is stopped and the registrant is informed.

[8] If the administration of the cryptographic module is carried out by the Registrant, the responsibility lies with the Registrant.

The RA will require the subscriber to sign a contract of personal assent to these responsibilities, as well as the assent of the licensees on whose behalf the subscriber is acting.

5.4.2.1 Approval of the application for the issuing of a certificate

Once the information provided by the subscriber has been validated, in case an application is approved by the RA, the registry operator will start the next process immediately:

a) Accessing a web system (Platform from now on) with access control and the protection of an SSL channel to be able to issue the certificate.
b) Authenticating on the Platform.
c) Starting the certificate issuance request.
d) Attaching electronically to the file the documents evidencing the verification of the holder from the previous step.
e) Requiring the signature of the subscriber's contract.
f) Issuing the certificate.

The profile that initiates this process ends with the issuing of the certificate.

Once the information provided by the subscriber has been validated, if the result of the validation is positive, the RA will send the respective ECD the authorisation to issue the certificate immediately.

In the event of a connection problem with the ECD, the maximum response time for the issuance of the certificate shall be five (5) days after the identity validation has been approved.

5.4.2.2 Rejection of the application for the issuing of a certificate

The application shall be rejected if the result of the validation carried out by the RA was negative, as set out in this document.

The EDC may decide to set out in its CPS or other relevant documentation additional circumstances for the rejection of the application, which will be assumed by the RA of the application.

5.4.3 Time to process requests for activation

Once the information required in the certificate request process has been verified, the required certificate may be issued. The maximum estimated service activation time after verification is 24 hours on working days.

Notwithstanding the fact that in the event of a connection problem with the ECD, the maximum response time for the issuance of the certificate shall five (5) days after the identity validation has been approved.

5.5 Activation of the services

All applications must be fully approved before the services are activated. Once the application has been approved, LLEIDANET will send the access credentials to the applicant to the email account indicated in the application process.

In particular, the process of issuing digital certificates securely binds the registration information and the generated public key.

The issued certificate is digitally signed by the issuing digital certificate service provider.

The subscriber will receive telematically the contract, the certification policy and certification practices specifying the conditions of use.

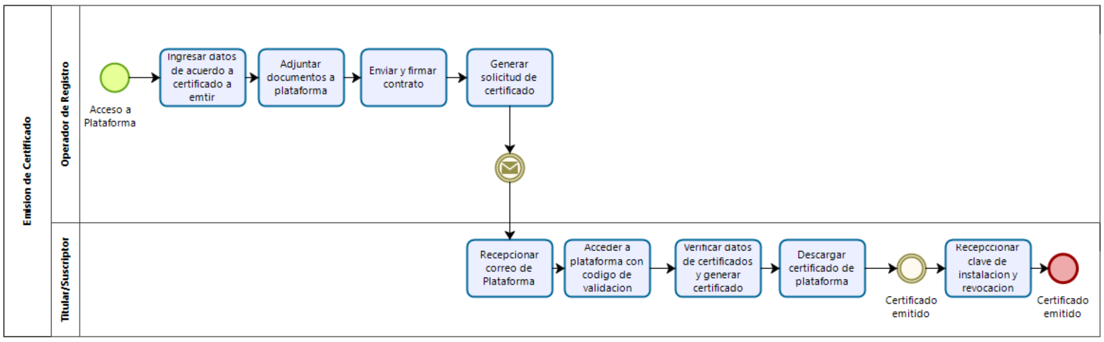
In any case, use of the services for this or any other purpose constitutes acceptance of the terms and conditions, the certification policy and the CPS

5.5.1 ECD shares during the issue

The issuing of the certificate will be carried out according to the selected means: software, hardware, via eSignalD or in the centralised signature service.

The generation of the key pair must be done in the presence and under the non-transferable responsibility of the subscriber. The secure request of the certificate to the ECD shall be made in the PKCS#10 format, thereby providing proof of possession of the private key.

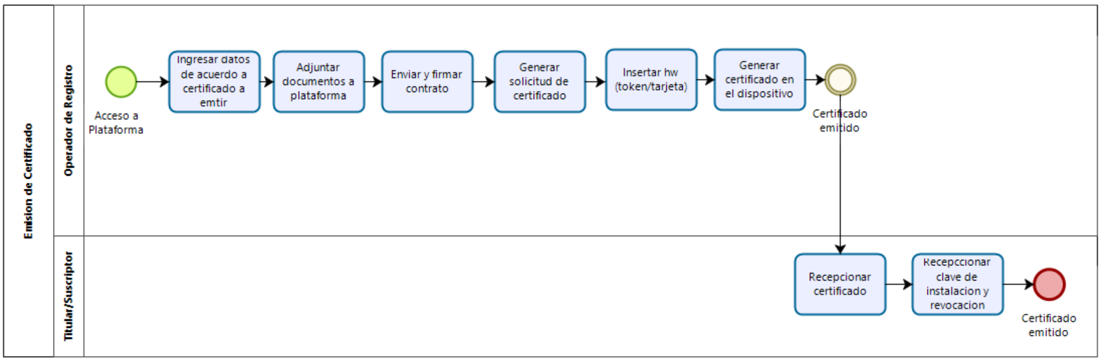
A. In the case that the issuance of the certificate is done in software, the process is as follows:


Emision de Certificado
Operador de Registro
Titular/Suscriptor
Acceso a Plataforma
Ingresar datos de acuerdo a certificado a emtir
Adjuntar documentos a plataforma
Enviar y firmar contrato
Generar solicitud de certificado
Recepcionar correo de Plataforma
Acceder a plataforma con codigo de validacion
Verificar datos de certificados y generar certificado
Descargar certificado de plataforma
Certificado emitido
Recepccionar clave de instalacion y revocacion
Certificado emitido

A link will be sent to the user by email that includes a validation code. Once the data is accessed and verified, the certificate will be generated, which can be downloaded and installed via a p12 or pfx file.

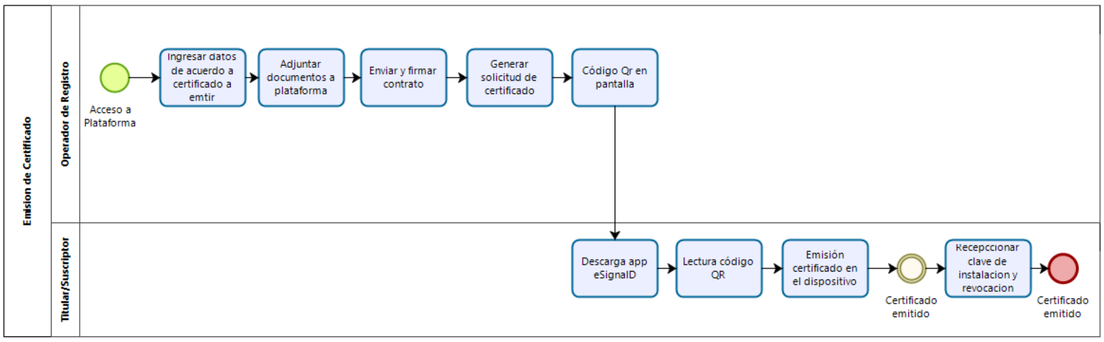
INFORMATIVE NOTE: All software certificates are issued in PKCS#12 format which is considered NOT ACCEPTABLE according to Annex G of the SPECIFIC CRITERIA FOR ACCREDITATION OF DIGITAL CERTIFICATION ENTITIES (CEA-3.0-07). These certificates are issued for those restricted domains that wish to accept them and are NOT ACCREDITABLE by ONAC.

B. If the certificate is issued by hardware, the process is as follows:


Emision de Certificado
Operador de Registro
Titular/Suscriptor
Acceso a Plataforma
Ingresar datos de acuerdo a certificado a emtir
Adjuntar documentos a plataforma
Enviar y firmar contrato
Generar solicitud de certificado
Insertar hw (token/tarjeta)
Generar certificado en el dispositivo
Certificado emitido
Recepcionar certificado
Recepccionar clave de instalacion y revocacion
Certificado emitido

In this case, the RA manages the cryptographic modules, so the devices delivered, be they tokens, cards or other, will comply at least with the FIPS 140-2 level 3 or Common Criteria EAL 4+ standards.

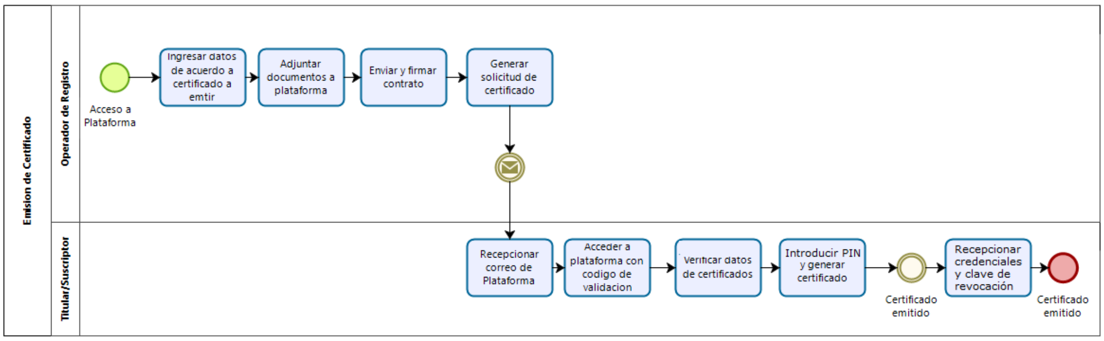
C. In the case of issuing the certificate using the eSignalD application, the process is as follows:



In the case of eSignalD, a QR code will be generated on the screen of the Registry Operator. In this case, the applicant installs the eSignalD application on his/her smartphone with which he/she reads the QR code. At this point the certificate will be generated on the smartphone.

In this case the RA does not manage any cryptographic module as the certificate is generated on the user's smartphone.

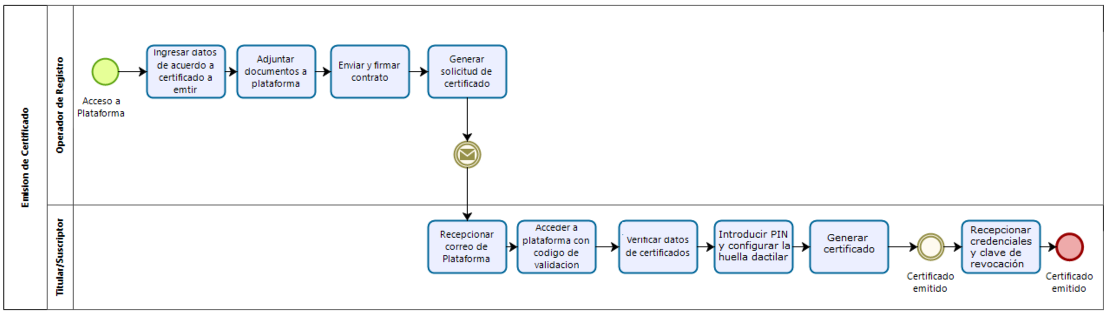
D. In the event that the certificate is issued in the centralised signature service with access via credentials, the process is as follows:


Emision de Certificado
Operador de Registro
Titular/Suscriptor
Acceso a Plataforma
Ingresar datos de acuerdo a certificado a emtir
Adjuntar documentos a plataforma
Enviar y firmar contrato
Generar solicitud de certificado
Recepcionar correo de Plataforma
Acceder a plataforma con codigo de validacion
Verificar datos de certificados
Introducir PIN y generar certificado
Certificado emitido
Recepcionar credenciales y clave de revocación
Certificado emitido

In this case of the centralised signature service using credentials, the applicant will receive an e-mail with a link to continue the certificate issuance process, in which they must enter a PIN that they will have to remember as it will be necessary later for the use of the generated certificate. In addition, they will receive other e-mails activating the certificate and with the credentials generated for accessing the certificate via the centralised signature service.

In this case the RA does not administer any cryptographic module as the certificate is generated in the ECD's centralised signature service.

E. If the certificate is issued in the centralised signature service with fingerprint access, the process is as follows:


Emision de Certificado
Operador de Registro
Titular/Suscriptor
Acceso a Plataforma
Ingresar datos de acuerdo a certificado a emtir
Adjuntar documentos a plataforma
Enviar y firmar contrato
Generar solicitud de certificado
Recepcionar correo de Plataforma
Acceder a plataforma con codigo de validacion
Verificar datos de certificados
Introducir PIN y configurar la huella dactilar
Generar certificado
Certificado emitido
Recepcionar credenciales y clave de revocación
Certificado emitido

In this case of the centralised signature service using a fingerprint, the applicant will receive an e-mail with a link to continue the certificate issuing process, in which they must enter a PIN that they will have to remember as it will be necessary later for the use of the generated certificate. Subsequently, the fingerprint will be configured for access to the certificate via the centralised signature service.

In this case the RA does not administer any cryptographic module as the certificate is generated in the ECD's centralised signature service.

5.5.2 Notification to the subscriber

The holder is informed of the issuance of their digital certificate by e-mail and therefore the applicant accepts and acknowledges that once the e-mail is received, the certificate shall be deemed to have been delivered. It shall be understood that the e-mail notifying the issuance of a certificate has been received when said e-mail enters the information system designated by the applicant, i.e. the e-mail address stated in the application form.

The publication of a certificate in the certificate repository constitutes proof and public notification of its issuance.

5.6 Acceptance of the certificate

5.6.1 Conduct constituting acceptance of the certificate

A certificate is accepted by the certificate holder from the moment it is downloaded or generated from the means offered by the ECD. Therefore, if the information contained in the issued certificate does not correspond to its current status or was not provided correctly, the applicant must request its revocation and the certificate holder accepts it, according to the procedure described in section 5.9.3 Certificate revocation request procedure in this document.

5.6.2 Publication of the certificate by the EDC

LLEIDA.NET publishes the certificates issued in a repository in X.509 V3 format and can be consulted on the website https://www.lleida.net/es/politicas-y-practicas where the certificate repository can be accessed.

5.6.3 Notification of the issue to other entities

LLEIDA.NET offers a system for consulting the status of certificates issued, on its website https://www.lleida.net/es/politicas-y-practicas. Accessing to this page is free of charge.

5.7 Key pair and use of services

5.7.1 Use of the subscriber's certificate and private key

The holder of the issued certificate and associated private key accepts the conditions of use established in this CPS by the mere fact of having requested the issuance of the certificate and may only use them for the uses explicitly mentioned and authorised in this CPS and in accordance with what is established in the "Extended Key Usage" fields of the certificates. Consequently, the issued certificates and the private key must not be used in other activities outside these uses. Once the validity of the certificate has expired, the certificate holder is obliged to stop using the private key associated to it. Based on the above, the holder accepts and acknowledges that, in this sense, he/she will be solely responsible for any loss or damage caused to third parties due to the use of the private key after the expiry of the certificate's validity. LLEIDA.NET assumes no liability for any unauthorised use.

The operator or subscriber shall notify the ECD or RA in the following cases:

1. The loss, theft or misplacement of the electronic security device that stores your private key (computer, cryptographic token or smart card).
2. The potential compromise of your private key.
3. Loss of control over the private key, due to compromise of activation data or any other cause.
4. Inaccuracies or changes in the content of the certificate known or likely to be known by the subscriber.

Likewise, the holder and subscriber shall cease to use the private key after the expiry of the certificate's validity period.

5.7.2 Use of the certificate and public key by trusted third parties

The certificate holder to whom a certificate has been issued is obliged to inform third parties each time he/she uses the certificate for third parties that it is necessary to consult the status of the certificate in the repository of revoked certificates, as well as in the repository of issued certificates, in order to verify its validity and that it is being applied within the permitted uses established in this CPS.

In this regard, they should check that:

- the associated certificate does not breach the validity start and end dates.
- the certificate associated with the private key is not revoked.

The relying third party shall comply with the following:

- Not to monitor, manipulate or reverse engineer the technical implementation of LLEIDA.NET, without prior written permission from the ECD.
- Not intentionally compromising the security of the LLEIDA.NET Hierarchy.
- Applying the appropriate verification criteria for the validation of a certificate during its use in electronic transactions.

Reporting any situation in which the ECD must revoke a certificate holder's certificate, provided that there is reliable evidence of compromise of the private key or illegal use of the private key. For example, you must report the loss, theft or misplacement of the electronic security device that stores a private key that does not belong to you (computer, cryptographic token or smart card).

5.8 Renewal of the services

LLEIDA.NET's digital certification services are automatically renewed, so if the user does not wish to use the service, he/she must inform the RA.

The certificate service is not automatically renewed and its renewal works according to the following paragraphs

5.8.1 Renewal of the certificate

5.8.1.1 Circumstances for the renewal of the certificate

For the Certification Authority LLEIDA.NET, a certificate renewal request is a normal request for a digital certificate as if it were a new one, and therefore implies a change of keys, which is recognised and accepted by the applicant.

The ECD. shall notify the subscriber at least 30 days before the expiry of the certificate, so that the subscriber can renew the certificate in time. If the subscriber does not request the certificate renewal, the certificate will expire. After that, the subscriber will have to go through the identity validation process from the initial stage.

5.8.1.2 Who can apply for the renewal of the certificate

Only certificate holders (natural person or legal entity) can apply for certificate renewal:

From natural person:

The application in the case of natural persons must be made by the same person who intends to hold the certificate.

From a legal person:

Both attribute certificates and certificates for automated agents, the application must be made by a representative appointed by the legal entity, who must submit to the RA Registration Agent, a document proving his powers as representative.

If, as part of the initial application, the representative has already been validated and registered by the RA of LLEIDA.NET, it will be sufficient to present their application signed by hand or with a digital signature to the Registration Agent. If the application is handwritten, the applicant must present their national identity document.

5.8.1.3 Processing of applications for renewal of certificates

5.8.1.3.1 Application for renewal of certificates

From natural person:

The applicant must apply in any of the service modalities specified in this document.

From a legal person:

- Application for renewal of attribute certificates
    - The applicant must specify in their application, the list of subscribers and the type of attribute to which each certificate corresponds, differentiating the legal representative of the legal entity from the workers who, as part of their position, require a digital certificate. This list must be duly signed by the Legal Representative or a person assigned by him/her.
- Application for renewal of certificates for automated agent

- If the certificate is intended for use by an automated agent, the application must be made by the designated representative of the legal entity that owns the device.
- The application shall specify the purpose of the certificate and the cryptographic module to be used.

5.8.1.3.2 Identification and authentication of certificate renewal applicants

From Natural Person:

It shall take place as described in section 4.2.3 Authentication of the identity of the natural person applying for this document.

From a legal person:

It shall take place as described in section 4.2.2 Authentication of the identity of an organisation (legal person) of this document.

5.8.1.3.3 Approval or rejection of the application for renewal of certificates

It shall take place as described in section 5.4.2 Approval or rejection of the certificate application of this document.

5.8.1.4 Notification of the renewal of the certificate

The holder is informed of the issuance of his/her digital certificate by e-mail and therefore the applicant accepts and acknowledges that once the aforementioned e-mail is received, the certificate shall be deemed to have been delivered. It shall be understood that the e-mail notifying the issuance of a certificate has been received when said e-mail enters the information system designated by the applicant, i.e. the e-mail address stated in the application form.
The publication of a certificate in the certificate repository constitutes proof and public notification of its issuance.

5.8.1.5 Conduct constituting acceptance of renewal with key generation

No confirmation is required from the certificate holder as acceptance of the certificate received. A certificate is accepted by the certificate holder from the moment it is requested to be issued, therefore, if the information contained in the issued certificate does not correspond to the current status of the certificate or was not correctly supplied, the certificate revocation must be requested by the applicant and the certificate holder accepts it.

The procedure for accepting the re-issuance of digital certificates is defined in the Registration Practice Statement of LLEIDA.NET as Registration Entity.

5.8.1.6 Publication of the renewed certificate

As with new certificates, the LLEIDA.NET Certification Authority publishes renewed certificates in a repository in X.509 V3 format and they can be consulted at https://www.lleida.net/es/politicas-y-practicas.

5.8.1.7 Notification of the renewal of the certificate to other entities

LLEIDA.NET notifies the renewal of the certificate to other entities according to section 5.6.3 Notification of issuance to other entities.

5.8.2 Renewal with regeneration of the certificate keys

For the Digital Certification Authority, a request for renewal of a certificate with key regeneration is a normal request for a digital certificate as if it were a new one, and therefore implies a change of keys, which is recognised and accepted by the applicant.
The ECD shall notify the subscriber, at least 30 days before the expiry of the certificate, so that the subscriber can renew the certificate in time. If the subscriber does not request the re-issuance of the certificate, the certificate will expire. After that, the subscriber will have to go through the identity validation process from the initial stage.

5.8.2.1 Circumstances for renewal with key regeneration

The circumstances for certificate renewal with key regeneration are carried out in the same way as explained in section 5.8.1.1 Circumstances for certificate renewal.

5.8.2.2 Who can apply for renewal with key regeneration?

This is done in the same way as explained in section 5.8.1.2 Who can request the renewal of the certificate.

5.8.2.3 Renewal application processing with key regeneration

This is done in the same way as explained in section 5.8.1.3 Processing of certificate renewal applications.

5.8.2.4 Notification of renewal with key regeneration

This is done in the same way as explained in section 5.8.1.4 Notification of certificate renewal.

5.8.2.5 Conduct constituting acceptance of renewal with key regeneration

This is done in the same way as explained in section 5.8.1.5 Conduct which constitutes acceptance of renewal with key generation.

5.8.2.6 Publication of the renewed certificate

This is done in the same way as explained in section 5.8.1.6 Publication of the renewed certificate.

5.8.2.7 Notification of renewal with key regeneration to other entities

This is done in the same way as explained in section 5.8.1.7 Notification of certificate renewal to other entities.

5.9 Modification of services

Any need for modification of certificates will imply a new application .

Digital certificates issued by the Digital Certification Authority cannot be modified. Instead, the holder must request the issuance of a new one. In this event and only once, a new certificate will be issued to the holder at no additional cost, for the time remaining until the original expiry date, charging only the value of the cryptographic device if applicable.

5.9.1 Circumstances for the amendment of the certificate

Not applicable as digital certificates issued by LLEIDA.NET cannot be modified.

5.9.2 Who can apply to amend the certificate

Not applicable as digital certificates issued by LLEIDA.NET cannot be modified.

5.9.3 Processing of certificate renewal applications

Not applicable as digital certificates issued by LLEIDA.NET cannot be modified.

5.9.4 Norification of the amendment of the certificate

Not applicable as digital certificates issued by LLEIDA.NET cannot be modified.

5.9.5 Conduct constituting acceptance of the amendment of the certificate

Not applicable as digital certificates issued by LLEIDA.NET cannot be modified.

5.9.6 Publication of the amended certificate

Not applicable as digital certificates issued by LLEIDA.NET cannot be modified.

5.9.7 Notification of the amended certificate to other entities

Not applicable as digital certificates issued by LLEIDA.NET cannot be modified.

5.10 Cancellation of services

The policies for each service set out the circumstances, requirements for applicants and the procedure for cancellation of services.

In particular, the revocation of certificates shall take into account the following points:

5.10.1 Circumstances for revocation of the certificate

The certificate holder acknowledges and accepts that certificates must be revoked when any of the following circumstances occur:

- Voluntary application by the Registrant.
- Voluntary or involuntary disclosure of the private key.
- Compromise of the Cardholder's private key due to loss, theft or damage.
- Loss, theft or damage to the physical device of the Certificate.
- Death of the holder, supervening disability, total or partial.
- Knowledge of events that modify the initial status of the data provided, among others: termination of the Legal Representation, termination of the employment relationship, liquidation and/or extinction of the legal status, cessation of the public function or change to a different one.
- At any time that there is evidence of falsity in the data provided by the applicant.
- Termination of activities of the certification service provider unless the issued certificates are transferred to another service provider.
- Compromise of the Certification Entity's private key due to loss, theft, robbery or damage.
- Loss, theft or damage of the physical device of the Certificate of the Certification Entity.
- Non-compliance by the Certification Body or the Holder of the obligations established in the Certification Practices Statement.
- Misuse of the holder's private key in accordance with the CPS.

    - By order of a court or competent administrative body.
    - For non-payment of the certification services agreed between the applicant and LLEIDA.NET.
    - By revocation of the powers of representation and/or powers of attorney of their legal representatives or proxies.
    - When the information contained in the certificate is no longer correct.
    - When the subscriber ceases to be a member of the community of interest or withdraws from those interests relating to the ECD.
    - When the subscriber or holder fails to comply with the obligations to which he/she is committed under the current regulations as stipulated in the subscriber's and/or holder's contract.
    - When the information contained in the certificate is no longer correct.
    - By decision of the respective legislation.
    - For any cause that reasonably leads to believe that the certification service has been compromised to such an extent that the reliability of the service is in doubt.
- In addition, the certificate of a certificate holder must be revoked by the ECD when:
    - Renewal of the certificate takes place.
    - Re-issuance of the certificate takes place.

Notwithstanding the above, LLEIDA.NET may also revoke certificates when, in its opinion, the credibility, commercial value, good name of ECD and/or the legal or moral suitability of the entire certification system may be jeopardised.

5.10.2 Who can request revocation of the certificate

The certificate holder, a Relying Third Party or any interested party when they have demonstrable knowledge of facts and grounds for revocation mentioned in the Circumstances for revocation of a certificate section of this CPS and which compromise the private key:

- The certificate holder or subscriber.
- The ECD that issued the certificate.
- A judge who in accordance with the law decides to revoke the certificate.
- A third party who has credible evidence of misuse of the certificate, key compromise or other ground for revocation referred to in the Act, the accreditation regulations and this document

The Security Committee, as the highest control body responsible for the administration of the security of the Certification Entity's technological infrastructure, is able to request the revocation of a certificate if it has knowledge or suspicion of the compromise of the subscriber's private key or any other event that tends to misuse the private key of the certificate holder or the Certification Entity.

5.10.3 Certificate revocation request procedure

Persons interested in requesting the revocation of a digital certificate for the reasons specified in this CPS may do so under the following procedures:

- Online revocation service. Through the LLEIDA.NET website, by accessing the digital certificate revocation service and authenticating the revocation PIN (CRIN), assigned during the digital certificate application process.
- Written requests for revocation of digital certificates signed by the certificate holders are received at the LLEIDA.NET offices during opening hours.
- Telephone Revocation Service. Through the permanent hotline, holders and third parties can request the revocation of digital certificates in accordance with the revocation grounds mentioned in the Circumstances for revocation of a certificate section of this CPS.
- Revocation Service via email. By means of our e-mail, holders and third parties can request the revocation of digital certificates in accordance with the grounds for revocation mentioned in the Circumstances for revocation of a certificate section of this CPS.

Revocation application procedures according to the type of applicant:

From natural person:

The applicant must apply in any of the service modalities specified in this document.

From a legal person:

For automated agent

In the event that the certificate is intended for use by an automated agent, the application must be made by the designated representative of the legal entity that owns the device.

5.10.4 Certificate revocation request grace period

Upon validation of the authenticity of a revocation request, LLEIDA.NET will immediately proceed with the requested revocation. Consequently, there is no grace period that allows the applicant to cancel the request. If it was a false alarm, the holder must request a new certificate, as the revoked certificate lost its validity as soon as the revocation request was validated.

The procedure used by LLEIDA.NET to verify the authenticity of a revocation request made by a specific person is to verify the request and validate it directly with the owner by contacting him/her and comparing the data provided in the original request.

Once the revocation of the certificate has been requested, if it becomes evident that said certificate is used in conjunction with the private key, the holder relieves LLEIDA.NET of all legal responsibility, as he/she acknowledges and accepts that the control, custody and confidentiality of the private key is the sole responsibility of the holder.

5.10.5 Deadline for processing the certificate revocation request

The request for revocation of a digital certificate shall be dealt with immediately using the procedure described in section 5.10.3 Certificate revocation request procedure of this document, which means that it shall be carried out in less than 60 minutes.

5.10.6 Obligation to verify revocations by relying parties

It is the responsibility of the holder of a digital certificate, and the holder accepts and acknowledges this, to inform the Third Parties they trust of the need to check the validity of the digital certificates they are using at any given time. The certificate holder shall also inform the relying third party that, in order to carry out this consultation, the list of revoked DPC certificates, published periodically by LLEIDA.NET at https://www.lleida.net/es/politicas-y-practicas, is available.

5.10.7 Frequency of CRL generation

Whenever a certificate revocation occurs, LLEIDA.NET will generate and publish a new CRL immediately in its repository and even if no revocation occurs, a new CRL will be generated and published every twenty-four (24) hours.

5.10.8 Maximum latency period of CRLs

The time between the generation and publication of the CRL is minimal due to automatic publication, less than 24 hours.

5.10.9 Availability of online certificate status verification system

LLEIDA.NET will publish both the CRL and the status of revoked certificates in freely accessible and easily consulted repositories, available 7X24 every day of the year. LLEIDA.NET offers an online consultation service based on the OCSP protocol at the address http://ocsp2.esigna.es.

5.10.10 Certificate revocation online verification requirements

To obtain information on the revocation status of a certificate at a given moment, the query can be made online at http://ocsp2.esigna.es. To do so, you must have software that is capable of operating with the RFC 6960 protocol. Most browsers offer this service.

5.10.11 Other forms of notice of revocation of compromised keys

The mechanisms that LLEIDA.NET makes available to users of the system will be published on its website https://www.lleida.net/es/politicas-y-practicas.

5.10.12 Special revocation requirements for compromised keys

If revocation of a digital certificate was requested due to compromise (loss, destruction, theft, disclosure) of the private key, the holder may request a new digital certificate for a period equal to or longer than that initially requested by submitting a renewal request in relation to the compromised digital certificate. The responsibility for the custody of the key is the responsibility of the holder and the holder accepts and acknowledges this, therefore, it is the holder who assumes the cost of the renewal in accordance with the current rates set for the renewal of digital certificates.

5.10.13 Circumstances for suspension

When a suspension occurs, LLEIDA.NET. will have one week to decide the definitive status of the certificate: (revoked or active). If LLEIDA.NET. does not have all the information necessary to verify its definitive status within this period, LLEIDA.NET. will revoke the certificate.

In the event of a certificate suspension, an email is sent to the Signatory/Subscriber informing the Signatory/Subscriber of the time of suspension and the cause of the suspension.

If the suspension does not lead to a definitive revocation and the certificate has to be activated again, the Signatory/Subscriber will receive an email indicating the new status of the certificate.

The suspension process does not apply to certificates

a. From TSU
b. From CA
c. From RA Agent
d. From OCSP

5.10.14 Who can apply for suspension

See section 5.10.2 Who can request revocation of the certificate

5.10.15 Procedure for requesting suspension

The suspension request shall be made by accessing the corresponding page on the LLEIDA.NET website or by means of a previously authenticated oral or written communication. The subscriber must have the revocation code to proceed with the suspension of the certificate.

5.10.16 Limits on the suspension period

A certificate shall not remain suspended for more than 7 days.

LLEIDA.NET will supervise, by means of a system of alerts on the certificate management platform, that the suspension period established by the corresponding Policies and this CPS is not exceeded.

5.11 Status of services services

The Certificate revocation status information allows users to know the status of the Certificate, not only until it expires, but also beyond that date, given that revoked certificates are not deleted from the corresponding CRL after they have expired. In the event of cessation of activity and/or compromise of the CA's keys, a final CRL will be generated, which will be kept complete and available for consultation, guaranteeing the availability of the certificate status information service for at least 15 years from its publication. The HASH of the file resulting from the CRL shall be indicated on the website: https://www.lleida.net/es/politicas-y-practicas, for verification when necessary.

The provision of information on the revocation status of the Certificates, in the event of LLEIDA.NET ceasing to operate as a Digital Certification Authority, is guaranteed by the transfer to the supervisory body or to another EDC with which the corresponding agreement is reached, of all the information relating to the Certificates and, especially, of the data on their revocation status.

When the infrastructure revokes a Certificate, the system reflects this fact in the database consulted by the Certificate Status Information and Query Service via the OCSP protocol, while generating a new CRL and publishing it in the repository. This database has a backup copy. In the event of any failure in the described sequence, an alarm is produced in order to correct the possible error. In this way, the consistency of the information supplied by these two methods (OCSP and CRL query) is guaranteed. Additionally, periodic monitoring of the repository is carried out as preventive maintenance.

The information relating to the verification of the revocation status of the electronic Certificates issued by LLEIDA.NET can be consulted by means of CRLs and/or the Certificate Status Information and Consultation Service by means of the OCSP protocol.

5.11.1Operational characteristics

To check the status of certificates issued by LLEIDA.NET, an online query service based on the OCSP protocol (Online Certificate Status Protocol: Protocol that allows the status of a digital certificate to be checked online) is available at the address http://ocsp2.esigna.es. The certificate holder sends a query request on the status of the certificate via the OCSP protocol, which, once the database has been consulted, is answered via http.

5.11.2 Service availability

The digital certificate status query service is available on the website 24 hours a day, every day of the year.

LLEIDA.NET will make every effort to ensure that the service is never continuously inaccessible for more than 24 hours, this being a critical service in LLEIDA.NET's activities and therefore treated appropriately in the Contingency and Business Continuity Plan.

5.11.3 Optional features

To obtain the certificate status information at a given moment, the query can be made online at the address http://ocsp2.esigna.es, for which you must have software that is capable of operating with the OCSP protocol. Most browsers offer this service.

5.12 END OF SUBSCRIPTION

The subscription is terminated at the request of the subscriber or for the reasons stated in this Certification Practice Statement.

The Digital Certification Authority terminates the validity of an issued digital certificate under the following circumstances:

- Loss of validity due to revocation of the digital certificate.
- Expiration of the period for which a certificate holder has contracted the validity of the certificate.

5.13 KEY ESCROW AND RETRIEVAL

5.13.1 Key Custody and Recovery Policies and Practices

The generation of the private key is the responsibility of the holder and is generated directly on a user-controlled device either in hardware or software format or with authentication mechanisms only available to the user in the case of a centralised signature, from which it cannot be exported. Consequently, recovery of the holder's private key is not possible because no copy exists. The responsibility for the custody of the private key is the responsibility of the holder and is accepted and acknowledged by the holder.

In the case of centralised signature, LLEIDA.NET stores the keys in secure HSM signature creation devices. The keys stored by LLEIDA.NET in its facilities have encryption mechanisms that only the user knows or has. LLEIDA.NET will not recover the private keys associated with the Centralised Signature Certificates. In the event of loss of the PIN that protects the Signatory's access to said Key, said Certificate must be revoked and a new one issued.

5.13.2Session Key Protection and Recovery Policies and Practices

The recovery of the holder's session code or PIN is not possible, as there is no copy of it, as the holder is the only one who can generate it and he/she declares and accepts it. The responsibility for the custody of the session key or PIN is the responsibility of the holder, who accepts not to keep digital records, written or in any other format, and who is obliged to memorise it, so forgetting it requires the request for revocation of the certificate and the request for a new one on behalf of the holder.

6 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

6.1 Physical checks

LLEIDA.NET is subject to the annual validations of the UNE-ISO/IEC 27001 standard, which regulates the establishment of suitable processes to guarantee the correct management of security in information systems.

LLEIDA.NET has established physical and environmental security controls to protect the resources of the facilities where the systems are located, the systems themselves and the equipment used for operations.

The physical and environmental security policy applicable to certified generation services provides protection against:

- Physical input controls
- Security of offices, offices and facilities
- Protection against external and environmental threats
- Working in safe areas
- Loading and unloading areas
- Siting and protection of equipment
- Supply facilities
- Wiring safety
- Maintenance of equipment
- Removal of company-owned materials
- Safety of off-site equipment
- Reuse or disposal of equipment
- Mobile device policy

6.1.1 Location and construction of facilities

LLEIDA.NET has the appropriate infrastructure to provide digital trust services at its facilities in Lleida.

For the certificate service infrastructure, LLEIDA.NET. has security measures in place to control access to the building where its infrastructure is located, as the digital certification services regulated and provided through this CPS are carried out by a service provider duly endorsed with ISO 27001 and ISO 20000. Only previously identified and authorised persons are allowed to enter the building with the visitor's card in a visible place.

This provider has a restricted area, physically separated from the other areas, with identified perimeters, where LLEIDA.NET's most sensitive operations are carried out and to which only authorised personnel have access.

This restricted area meets the following requirements:

- It is completely isolated from the other areas.
- Only authorised persons may enter.
- Mission critical equipment is adequately protected in racks.
- There are no windows to the outside of the building.
- It has a 24-hour closed-circuit television system with cameras both inside and outside the computer centre.
- It has card-based access control and biometric reader.
- Fire protection and fire prevention systems: smoke detectors, fire extinguishing system.
- It has trained personnel to respond to catastrophic events.
- It has an intruder detection system
- The cabling is adequately protected against damage, sabotage or interception by means of cable ducts.
- It is separated from loading and unloading areas.
- There is no frequent traffic of people in the vicinity.

6.1.1.1 Status of the Data Processing Centre

It is specified in the document: DOC-1792117 - CPS Indenova Technical Dossier.

6.1.2 Physical access

LLEIDANET's facilities have a complete physical access control system consisting of:

- Perimeter security to prevent unauthorised access.
- Control over physical access to the installation.
  - Only authorised personnel are allowed access.
  - Access rights to the security area are regularly reviewed and updated.
  - All personnel must be identified and it is not possible to circulate in the building without being identified and accompanied by an employee.
  - Staff who are not on the LLEIDA.NET access list and who may be working on the site are properly supervised.
- Access to the facilities housing the servers involves video recording of activity and requires biometric identification and dual access control.
- Access to the premises hosting the servers is logged.
  There are additional measures to limit access to the building at the LLLEIDANET offices.
- The RAs comply with the necessary security criteria defined in the registration site's securitisation document.

Access to the systems that provide digital certification services is protected with 3 levels of access: Office, DPC and server access.

Access to the office area and meeting rooms by external personnel is controlled by means of a visitors' register.

The technical details of the certificate service infrastructure are specified in the document: DOC-1792117 - CPS Indenova Technical Dossier.

6.1.3 Electricity and air conditioning

The data processing centre has sufficient power and air conditioning to create a reliable operating environment.

All servers in all data centres are equipped with uninterruptible power supply systems (UPS) that ensure that services are not interrupted in the event of occasional drops in the electricity supply (micro cuts) or that equipment is not damaged in the event of unexpected power surges. They also provide a certain degree of autonomy in the event of a longer power outage (between 15 and 30 minutes depending on the case).

A dedicated generator set is available at the head office to enable the operation of services in the event of a longer power failure. A maintenance contract is in place to ensure availability and refuelling.

In the secondary data centre there is also a generator set that allows the operation of the services in the event of a longer power failure.

With regard to the certificate service infrastructure, the computer centre has an air-conditioning system and an adequate electricity supply with protection against voltage drops and other electrical fluctuations that could eventually have a significant impact on the equipment and cause serious damage. In addition, there is a back-up system to ensure that there is no interruption in service with sufficient autonomy to guarantee continuity of service. In the event of a failure in the backup system, there is sufficient time for a controlled shutdown.

6.1.4 Exposure to water

LLEIDA.NET has taken the necessary precautions to minimise the impact of exposure to water. Its facilities are located in a geographically elevated location.

With regard to the certificate service infrastructure, the computer centre is isolated from potential water sources and has flood detection sensors connected to the general alarm system.

6.1.5 Fire prevention and protection

The LLEIDA.NET data processing centre has physical barriers extending from the floor to the ceiling, as well as automatic fire detection systems for the purpose of:

- Notifying the security guards and LLEIDA.NET staff of the start of a fire.
- Switch off the ventilation system, close the fire doors, switch off the power supply and activate the automatic fire extinguishing system.

In addition, fire extinguishers are equipped with signposted fire extinguishers.

6.1.6 Media storage

Media containing backup information is securely stored in a separate data centre with the necessary security measures.

6.1.7 Waste disposal

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

Storage media containing confidential information is destroyed to ensure that the data is not readable or recoverable after deletion.

6.1.8 External backup

LLEIDA.NET keeps backup copies of the storage media in a safe and accident-protected environment and at a sufficient distance to prevent damage in the event of a disaster at the original site.

6.2 Procedural controls

6.2.1 Trusted roles

A "trusted role" is defined as functions assigned to an individual that may lead to security problems if not performed satisfactorily, either accidentally or intentionally.

To ensure that trusted roles adequately fulfil their duties, the following considerations are addressed:

- First, the technology is designed and configured to prevent errors and inappropriate behaviour.
- Second, the tasks are distributed among several individuals so that any misconduct would require the complicity of several of them.

LLEIDA.NET has complete definitions of all the functions performed in the organisation. The duties and responsibilities associated with each function are defined, and each has a set of documented procedures that regulate the practice attached to each one.

For the operation of the system, the following trust roles have been defined within the digital certificate issuance system:

- System Administrator: Responsible for activities related to the installation, configuration and maintenance of the hardware and software infrastructure.
- Service Administrator: Responsible for monitoring availability, health status and managing access to the services offered by the PKI platform, including the periodic review of audit logs.
- Internal Auditor: Responsible for auditing the processes of the digital certificate issuance cycle and ensuring compliance with information security procedures and policies.
- RA Operator: Responsible for verifying that the information provided by digital certificate applicants is authentic and complete. It is responsible for requesting the issuance or revocation of digital certificates on behalf of the certificate holders.
- Responsible for the SGSI: Responsible for coordinating, controlling and enforcing the security measures defined by the security policies of INDENOVA S.L. He/she must be in charge of aspects related to information security: logical, physical, network, organisational, etc.
- DPC Provider: Responsible for the Data Centre and remote hands[9] to the EDC systems.

6.2.2 Number of persons required per task

Several persons can be assigned to the same function.

The ECD guarantees the collaboration of at least two people to carry out the tasks that affect the cryptographic key management of the ECD itself.

6.2.3 Identification and authentication for each post

Trusted roles require verification of identity by secure means. All trusted roles are performed by individuals.

Each person only controls the assets necessary for their role, thus ensuring that no one person accesses unallocated resources.

The System Administrator, Service Administrator, Internal Auditor, ER Operator and ISMS Manager are authenticated by digital certificates issued by INDENOVA S.L. or by login/password.

LLEIDA.NET has specific documentation that gives more details of each function.

[9] This service shall be used in exceptional cases and with the authorisation of the PKI manager.

6.3 Personnel controls

6.3.1 Background, qualifications, experience and application requirements

LLEIDANET employs staff with the necessary experience and qualifications to carry out their job responsibilities.

All personnel in positions of trust are free from any interest that may affect their impartiality with respect to the operations of LLEIDA.NET.

6.3.2 Training requirements

LLEIDA.NET provides its staff with the necessary training to carry out their job responsibilities competently and satisfactorily. Staff training includes the following:

- A copy of the Certification Practice Statement.
- Awareness raising and training on information security
- Security procedures for each specific function.
- Management and operating procedures for each specific function.
- Disaster recovery procedure.
- Incident management procedure

The applicable security requirements include those set out in the Information Security Management System developed in the framework of the ISO 27001 certification.

6.3.3 Frequency and requirements of further training courses

Any significant change in the operations of LLEIDA.NET digital certification services will require a training plan and the implementation of the plan will be documented.

6.3.4 Job rotation and sequencing

There is no rotation of tasks in positions of trust.

6.3.5 Sanctions for unauthorised actions

Information security incidents. LLEIDA.NET has a security incident management plan that has been designed taking into account the provisions of ISO 27001.

Sanctions for unauthorised actions. There is an internal disciplinary regime that defines the sanctions applicable to staff depending on the seriousness of the actions.

6.3.6 Recruitment requirements for staff

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

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

It also expresses its commitment to work to guarantee the accessibility of its services and facilities to all people, regardless of their technical, cognitive or physical abilities.

Employees hired to perform trusted tasks previously sign the confidentiality clauses and operational requirements employed by LLEIDA.NET. Any action that compromises the security of the accepted processes could, upon evaluation, result in the termination of the employment contract.

6.3.6.1 Third party contracting requirements

Among the requirements for contracting third parties is the knowledge of the Security Policies and the signing of a Confidentiality Agreement on the information that is supplied or known.

6.3.7 Documentation provided to staff

All staff in positions of trust receive:

- A copy of the Certification Practice Statement
- A copy of the Handbook which includes specific confidentiality and security considerations.
- Documentation defining the duties and procedures associated with each role.
- Staff also have access to the operating manuals of the various components of the system.

6.4 Audit logging procedures

Audit logs are used to reconstruct significant events recorded in the LLEIDA.NET or Registration Authority system and the user or event that gave rise to the record. The logs will also be used in arbitration to resolve any possible conflict by checking the validity of a signature at a given point in time.

6.4.1 Types of registered events

LLEIDANET records and stores audit trails of all events related to the ECD's security system.

The following events will be recorded:

- Switching the system on and off.

- Attempts to create, delete, set passwords or change privileges.
- Login and logout attempts.
- Attempts to gain unauthorised access to the ECD system via the network.
- Unauthorised access attempts to the file system.
- Physical access to audit trails.
- Changes in system configuration and maintenance.
- ECD application records.
- Switching the ECD application on and off.
- Changes to the details of the ECD and/or its keys.
- Changes in the creation of service policies.
- Records of destruction of media containing keys, activation data.
- EC key generation.
- Null read and write attempts on a certificate and in the repository.
- Certificate lifecycle events: issuance, revocation, reissuance, suspension and modification

LLEIDA.NET also keeps, either manually or electronically, the following information:

- Physical access records.
- Maintenance and system configuration changes.
- Commitment and discrepancy reports.
- Records of the destruction of material containing key information, activation data or personal information of the Signatory, in the case of individual certificates, or of the key holder, in the case of organisational certificates.
- Possession of activation data, for operations with the Certification Entity's private key.
- Comprehensive reports of attempts of physical intrusion into the infrastructures supporting the issuance and management of digital certification services.

The most sensitive activities of the certification cycle require the control and monitoring of events that may occur during their operation. According to their level of criticality, events are classified as follows:

- Informative: an action ended successfully.
- Type of marking: start and end of a session
- Warning: presence of an abnormal event but not a failure.
- Error: an operation generated a predictable failure.
- Fatal error: an operation generated an unpredictable failure.

6.4.2 Frequency of register processing

Audit records are regularly reviewed by the LLEIDANET auditor.

Log reviews are performed when a security alert is detected or there are indications of unusual system operation.

6.4.3 Audit trail retention period

LLEIDA.NET stores audit trail information depending on the nature of the audit records.

Auditors have a right of access to audit records.

Unauthorised deletion or modification of log entries is prevented by writing audit trails using media not suitable for rewriting or deletion without detection.

LLEIDA.NET stores the information from the audit records of the certificate system for at least fifteen (15) years.

6.4.4 Protection of audit trails

Unauthorised deletion or modification of log entries is prevented by writing audit trails using media not suitable for rewriting or erasure, such as CD-ROM or other media.

6.4.5 Backup procedures for audit trails

Backup management systems are among the security measures adopted by the institution.

When there is any ECD management, the previous situation is backed up. There will always be a backup of the last modification, and, if necessary, in separate locations from where the service is provided.

6.4.6 Audit Information Gathering System

Audit trails and their back-up are obtained on a daily basis, usually automatically.

6.4.7 Notification to the subject cause of the event

In general, there is no procedure for notifying the subjects of audit events in any of the collection scenarios, neither in the automatic nor in the manual one.

In the certificate issuance system, at the discretion of the Security Committee, the subject shall be notified of a security incident detected through the audit logs in order to have a formal response on what happened.

6.4.8 Vulnerability assessments

Vulnerability analysis is covered by LLEIDA.NET's auditing processes.

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

This document specifies the controls in place to ensure the required security objectives.

In addition, White Hat Ethical Hacking or Penetration Testing audits are outsourced.

6.5 Archive of information and records

6.5.1 Type of information and events registered

LLLEIDA.NET keeps the following documents involved in the life cycle of the services:

- All system audit records detailed in section 6.4 of this certification practice statement.
- The various versions of the Certification Practice Statement
- The Certification Policies in their different versions
- Requests for activation and deactivation of services.
- Identity of the Registration Entity accepting the certificate application.
- Documentation collected by the LLEIDA.NET Registration Entity
- Service lifecycle information.
- Contracts with clients requesting services
- Contracts with third parties for the provision of services

6.5.2 Retention period for the archive

In accordance with current legislation, LLEIDA.NET will keep all information and documentation relating to the services and certification practice statements for 5 years.

The retention period for this type of documentation for the certificate service is fifteen 15 years.

6.5.3 File protection

LLEIDA.NET establishes controls, policies and procedures that guarantee the integrity of the documentation and access only by authorised personnel.

Storage is carried out in a place with appropriate security controls.

6.5.4 Archive backup procedures

LLEIDA.NET periodically backs up the information, at least on a daily basis.

6.5.5 Requirements for time-stamping of records

The information is dated by a reliable time source. No electronic signature is used for this purpose.

6.5.6 Audit information collection system

LLEIDA.NET uses an internal system for collecting and storing information in accordance with its procedure within the framework of ISO 27001.

6.5.7 Procedures for obtaining and verifying archived information

LLEIDA.NET within the framework of ISO 27001 has procedures to verify the integrity of the information stored.

Access is only possible for authorised personnel.

6.6 Change of keys

6.6.1 Change of root keys

The Root key change procedure is the equivalent of generating a new digital certificate. The certificates issued by the subordinate ECDs with the previous key must be revoked or the infrastructure must be maintained until the expiry of the last certificate issued. If it is decided to revoke the certificates and issue new ones, these will be free of charge for the certificate holder.

Before the use of the ECD's private key expires, a key exchange will take place. The old ECD and its private key shall only be used for signing the CRL as long as there are active certificates issued by the subordinates of the old ECD. A new ECD shall be generated with a new private key and a new DN. The public key will be published in the same repository with a new name that differentiates it from the old one.

6.6.2 Change of keys of a subordinated ECD

The key change procedure of a subordinate ECD is the equivalent of generating a new digital certificate. Certificates issued with the previous key of the subordinate must be revoked or the infrastructure must be maintained until the expiry of the last certificate issued. If it is decided to revoke the certificates and issue new ones, these will be free of charge for the certificate holder.

Before the use of the private key of the ECD Subordinate expires, a key exchange shall take place. The old ECD subordinate and its private key shall only be used for signing the CRL as long as there are active certificates issued by the old ECD subordinate. A new ECD subordinate shall be generated with a new private key and a new DN. The public key will be published in the same repository with a new name that differentiates it from the old one.

6.7 Recovery in case of service compromise or disaster

6.7.1 Incident management procedures and commitments

LLEIDA.NET has internal procedures in place for the management of security incidents and incidents that may compromise the security of the information stored that allow them to manage various incidents, in particular:

- that the certification body's security system has been breached;

- that failures occur in the certification authority's system that compromise the provision of the service;

- that the encryption systems become invalid because they do not offer the level of security contracted by the subscriber.

6.7.2 Corruption of resources, applications or data

In case of corruption of resources, applications or data, the corresponding incident management processes are activated to enable detection, investigation, correction and timely communication to the affected actors.

Depending on the type of incident, business continuity procedures may be activated.

6.7.3 Procedure in the event of compromise of the entity's private key

LLEIDA.NET Certification Authority has established a Contingency Plan that defines the actions to be taken in the event of a vulnerability of the private key of the root of LLEIDA.NET or one of its subordinate CAs. In these cases, the compromised private keys of LLEIDA.NET and the certificates signed under its hierarchy must be immediately revoked. A new private key must be generated and new certificates must be issued at the request of the holders.

In case of commitment of the ECD the Certification service provider:

> It shall inform all Data Subjects, Relying Parties and other CCPs with which it has agreements or other relationships of the commitment.

It shall indicate that certificates and revocation status information signed using this key are invalid.

6.7.4 Business continuity after a disaster

The Business Continuity Plan guarantees recovery in the event of a disaster. Depending on the criticality of the affected systems the recovery time can be up to 24 hours. The accredited services will maintain an availability of 99.8% 7x24x365 per year.

6.8 Termination or cessation of the ECD or RA

6.8.1 Certification Authority

LLEIDANET has an ECD Termination Plan that specifies the procedure to be followed in case such an event occurs.

LLEIDA.NET shall duly inform the Subscribers and Certificate Holders, as well as the Users of the affected services, of its intentions to terminate its activity as a Trusted Service Provider at least two (2) months prior to the cessation of this activity.

Any subcontracting aimed at providing functions on behalf of LLEIDA.NET for the service to be terminated shall be terminated.

Once the absence of opposition from the Subscribers has been accredited, it may transfer those Certificates that are still valid on the effective date of cessation of activity to another Trusted Service Provider that assumes them. If this transfer is not possible, the Certificates shall expire.

Whatever the service being terminated, LLEIDA.NET will transfer to a third party the event logs, registration information, revocation and audit status information, as well as the Certificates used in the provision of the service, for a period of time sufficient for the purposes dictated by current legislation.

It shall notify the Supervisory Body of the cessation of its activity and the destination it is going to give to the Certificates, specifying if applicable: if it is going to transfer them, to whom, or if it is going to cancel them. The notification to said body shall be made at least two (2) months in advance, in a handwritten or electronically signed document. In addition, the information relating to the Certificates whose validity has been terminated shall be sent to the aforementioned body so that it may take custody of them for the pertinent purposes.

It will transfer its obligations regarding the maintenance of registration information and logs for the indicated period of time to subscribers and users.

Private Keys shall be destroyed so that they cannot be recovered.

6.8.2 Registration authority

After a Registration Authority ceases its operations, it will transfer to LLEIDA.NET the records relating to the identification of applicants for services and audit trails.

All other information will be deleted and destroyed.

7 SECURITY ENGINEERING CONTROLS

7.1 Key pair generation and installation

7.1.1 Key pair generation

7.1.1.1 ECD key pair generation

The generation of the Root ECD key pair was carried out in the cryptographic room of the ECD/RA platform service provider with the strictest security measures and under the key generation ceremony protocol established for this type of event and in the presence of the legal representative of the Certification Body LLEIDA.NET. A FIPS 140-1 level 3 or Common Criteria EAL 4+ approved cryptographic device with dual control was used to store the private key.

7.1.1.2 RA key pair generation

The generation of the key pair of the LLEIDA.NET subordinate CIs is carried out within the cryptographic room of the LLEIDA.NET service provider under the key generation ceremony protocol. A FIPS 140-1 level 3 or Common Criteria EAL 4+ approved cryptographic device with dual control is used to store the subordinate private key.

7.1.1.3 Generation of the subscriber key pair

The generation of the key pair is generated directly by the subscriber, using a secure cryptographic device "Hardware Security Module (HSM)" for secure key generation and transmitted through a secure channel; or by means of a protected file using the PKCS#12 standard.

7.1.2 Sending the private key to the subscriber

The private key is generated by the holder in his cryptographic device and cannot be extracted. There is therefore no copy of the holder's private key.

7.1.3 Sending the public key to the certificate issuer

The public key is sent to the ECD as part of the digital certificate request in PKIX-CMP format.

7.1.4 CA public key distribution to relying parties

The public key of the Root ECD and the Subordinate ECD is included in its digital certificate.

The ECD Root certificate can be consulted by trusted third parties at https://certs.esigna.es/root/ca_root_lleidasas.crt.

The certificate of the Subordinated ECD can be consulted by trusted third parties at https://certs.esigna.es/ca/lleidasas_pki_001.crt.

7.1.5 Key sizes and algorithms used

The key size of the LLEIDA.NET Root EC is 4096 bits.

The key size of the LLEIDA.NET Subordinates is 4096 bits.

The key size of the certificates issued by LLEIDA.NET to end users is 2048 bits.

When trying to derive the private key from the 2048-bit public key contained in end-user certificates, the problem lies in finding the prime factors of two large numbers, as there would be 2^{2047} possibilities for each number. It is currently computationally impossible to factor these numbers in a reasonable time. It is estimated that decrypting a 2048-bit public key would require processing work in the order of 3 x10^{20} MIPS-10[10] .

In any case, LLEIDA.NET keeps itself informed of existing technologies and in the event that the encryption systems become obsolete due to the appearance of new technologies, measures will be taken immediately to restore the reliability of the system, modifying this CPS accordingly.

[10] MIPS-year: unit used to measure the processing power of a computer running for one year. It is equivalent to the number of millions of instructions a computer is capable of processing per second during a year.

7.1.6 Public key generation parameters and quality check

The public key of the Root CA is encrypted according to RFC 5280 and PKCS#1. The signature algorithm used in the generation of the keys is RSA.

The public key of the LLEIDA.NET subCAs is encrypted according to the RFC 5280 standard and PKCS#1. The signature algorithm used in the generation of the keys is RSA.

The public key of the end-user certificates is encrypted in accordance with the RFC 5280 standard and PKCS#1. The signature algorithm used in the generation of the keys is RSA.

7.1.7 Permitted uses of the keys

The permitted uses of the key for each type of certificate are established by the Certification Policy defined for each type of certificate issued by the LLEIDA.NET Certification Authority.

All digital certificates issued by the LLEIDA.NET Certification Authority contain the 'Key Usage' extension defined by the X.509 v3 standard, which is classified as critical.

TYPE OF CERTIFICATE	KEY USAGE
Signature Certificate	Digital Signature
Authentication Certificate	Non Repudiation

7.2 Private key protection in cryptographic module

7.2.1 Standards for cryptographic modules

The cryptographic modules used in the creation of keys used by LLEIDA.NET Certification Entity Root CAs comply with the requirements established in accordance with ITSEC, Common Criteria EAL 4+ or FIPS 140-2 Level 3 or higher security level.

7.2.2 Multi-person (n of m) control of the private key

The private keys, of LLEIDA.NET Root and the private keys of the subordinates of, are under multi-person control. The method of activation of the private keys is by initialisation of the LLEIDA.NET software by means of a combination of keys held by several operators.

7.2.3 Custody of the private key

The private keys of the LLEIDA.NET Certification Authority are stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria EAL 4+ or FIPS 140-1 Level 3 or higher security level.

The technical data of the device are as follows:

- nShield F3 ready, 500 TPS

-PCI connectivity , FIPS 140-2 level 3 Common Criteria EAL 4+ certified, with SEE (Secure Encryption Engine) and ECC (Elliptic Curve Cryptosystem) cryptography capabilities.

The private key of end-user digital certificates is under the exclusive control and custody of the holder. Under no circumstances does LLEIDA.NET keep a copy of the holder's private key, as this is generated by the holder and cannot be accessed by LLEIDA.NET.

The devices used are classified as qualified devices included in the list published by the member states of the European Commission.

And before any change of model or purchase of a new device, a check is carried out to ensure that the device is qualified and included in the list published by the member states of the European Commission.

In the event of loss of QSCD certification of any of the qualified signature/seal creation devices used by LLEIDA.NET as Digital Certification Authority, the appropriate measures will be taken to minimise the possible impact, informing the supervisory body and stopping the issuing of certificates on these devices. Subscribers will also be notified of the revocation of the certificate, stating the reason for the loss of QSCD certification and will be informed of the possibility of reissuing the certificate on a device that complies with QSCD certification.

7.2.4 Backup of the private key

The private keys of the LLEIDA.NET Certification Authority are stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria EAL 4+ or FIPS 140-1 Level 3 or higher security level (see Custody of the private key).

Backup copies of LLEIDA.NET private keys are stored on external devices cryptographically protected by a dual control and are only recoverable within the same device on which they were generated.

7.2.5 Archiving of the private key

The private keys of the LLEIDA.NET Certification Authority are stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria EAL 4+ or FIPS 140-1 Level 3 or higher security level (see Custody of the private key).

The archive of the backup copies of the private keys is archived in the safe deposit box of an external centre.

Private keys used for the signature and authentication of end-users, as well as electronic files containing them (e.g. files with extension PFX), shall not be archived.

7.2.6 Transfer of the private key to the cryptographic module

The private keys of the LLEIDA.NET Certification Authority are stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria EAL 4+ or FIPS 140-1 Level 3 or higher security level (see Custody of the private key).

The downloading process of the private keys is performed according to the procedure of the cryptographic device and they are securely stored protected by cryptographic keys with dual control.

7.2.7 Storage of the private key in the cryptographic module

The private keys of the LLEIDA.NET Certification Authority are generated and stored in cryptographic devices that meet the requirements established in accordance with ITSEC, Common Criteria EAL 4+ or FIPS 140-1 Level 3 or higher security level (see Custody of the private key).

Cryptographic keys can be loaded into a cryptographic device of equal performance from backup copies by a process that requires the participation of at least two operators.

7.2.8 Method of activating the private key

The private keys of LLEIDA.NET Root and Subordinate CAs are under multi-person control. The method of activation of the private key is by initialisation of the LLEIDA.NET software by means of a combination of keys held by several operators.

Multi-person control is required for ECD private key activation. At least 2 out of 4 persons are required for key activation.

7.2.9 Private key deactivation method

The deactivation of the private key is done by deactivating the software and/or shutting down the ECD server. It is reactivated by using multi-person control, following the procedures laid down by the manufacturer of the cryptographic module.

7.2.10Method of destruction of the private key

The method used in case destruction of the private key is required is by erasing the keys stored in the cryptographic devices as described in the device manufacturer's manual and physically destroying the access cards held by the operators.

7.2.11Classification of cryptographic modules

The cryptographic device is monitored by its own software to anticipate possible failures.

7.3 Other aspects of key pair management

7.3.1 Public key file

The EDC shall keep its archives for a minimum period of fifteen (15) years as long as the technology at any given time allows it. The documentation to be kept includes the public key certificates issued to its subscribers and its own public key certificates.

7.3.2 Period of use for public and private keys

The period of use of the key pair is determined by the validity of the certificate.

The period of validity of the digital certificate and the key pair of the Certification Authority's Root CA and LLEIDA.NET's Subordinate CAs is thirty (30) years.

7.4 Activation data

7.4.1 Generation and installation of activation data

For the operation of the Certification Authority, cryptographic cards are created for the operators of the cryptographic device, which, together with a PIN, will be used for the activation of the private keys.

The private key activation data is divided into cryptographic cards guarded by a multi-person system where 4 persons share the access code of these cards.

7.4.2 Activation data protection

Knowledge of the activation data is personal and non-transferable. Each participant is responsible for its safekeeping and must treat it as confidential information.

7.4.3 Other aspects of activation data

The activation key is confidential, personal and non-transferable and therefore security rules for its safekeeping and use must be taken into account.

7.5 Computer security controls

7.5.1 Specific technical requirements for computer security

There are a series of controls in the different components that make up the system for the provision of LLEIDANET services (LLEIDANET databases, LLEIDANET Internet services, ECD operation and network management):

- Operational controls

    - All operational procedures are duly documented in the corresponding operations manuals. LLEIDANET maintains a contingency plan.
    - Tools have been implemented to protect against viruses and malicious code.
    - Equipment is continuously maintained to ensure uninterrupted availability and integrity.
    - A procedure is in place to securely store, erase and dispose of obsolete storage media, removable media and equipment.
- Data exchange. Data exchanges are encrypted to ensure confidentiality.
    - Transmission of pre-registration data.

- Access control
    - Unique user IDs are used in such a way that users are associated and can be held accountable for their actions.
    - Rights are assigned according to the rule of providing users with the least amount of system privileges they need to do their work.
    - Access rights are immediately cancelled when users change jobs or leave the organisation.
    - The level of access assigned to users is reviewed every three months.
    - System privileges are assigned on a case-by-case basis and terminate once the reason for their assignment is no longer valid.
    - LLEIDANET maintains password quality guidelines.

7.5.2 Assessment of the level of IT security

The information security management system evaluates the processes related to the technological infrastructure in order to identify possible weaknesses and define continuous improvement plans with the support of permanent and periodic audits.

The security of equipment is reflected by an initial risk analysis such that the security measures implemented are in response to the likelihood and impact when a defined set of threats can exploit security breaches.

This analysis is carried out on an ongoing basis so that new vulnerabilities in the systems are identified.

7.6 Life cycle engineering controls

7.6.1 System development controls

The implementation of software for production systems is monitored.

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

- There is a formal authorisation procedure for updating software libraries (including patches) in production. Authorisation is granted only after ensuring that it works properly.
- The test system is kept separate from the production system to ensure that it is working properly before going into production.
- A log file is kept on all library updates.

- Previous versions of the software are retained.
- The purchased software is maintained at the level supported by the supplier.
- Procedures are in place to include extensions to the source code.

7.6.2 Security management controls

LLEIDANET carries out internal and external audits to check the correct application of its policies. These include:

- Audit against ISO 27001;
- Ethical hacking audits (penetration tests);
- Audits against the eIDAS standard.

7.6.3 Life cycle security controls

In order to perform tests, a large volume of data as similar as possible to production data is required. LLEIDANET avoids the use of production databases with personal information.

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

7.7 Network security controls

LLEIDA.NET has a network infrastructure properly monitored and equipped with security elements required to ensure high availability and confidence in the services offered to its owners and third parties who trust.

Information related to Information Security is considered confidential and therefore can only be provided to those accredited bodies that require knowledge of it.

7.8 Time sources

The servers are kept up to date with UTC time. They are synchronised via NTP (Network Time Protocol).

8 CERTIFICATE AND CRL PROFILES

8.1 Certificate profile

The certificates comply with the X.509 version 3 standard and for the authentication infrastructure it is based on RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Contents of the certificates. A certificate issued by LLEIDA.NET, in addition to being digitally signed by LLEIDA.NET, will contain at least the following:

1. Name, address and domicile of the holder.

2. Identification of the holder named in the certificate.
3. The name, address and place of business of the certification body.
4. The user's public key.
5. The methodology for verifying the digital signature of the holder, imposed on the data message.
6. The serial number of the certificate.
7. Date of issue and expiry of the certificate.

- For natural persons

The identification of the holder involves the ID card number and the type of document plus the first and last name

- For certificates of natural persons linked to a legal person (certificates of legal representative, company membership or electronic seal)

The name and identification of the holder implies the following: tax identification number of the organisation, name of the company name and name and surname of the subscriber.

Description of the content of the certificates

Field	Value or restrictions
Version	V3 (X.509 version 3)
Serial Number	Unique identifier issued by LLEIDA.NET
Signature Algorithm	SHA1RSA

Emitter	See section "Rules for the interpretation of various forms of names".
	For LLEIDA.NET as issuer is specified:
	Description =Lleida SAS Subordinate CA CO 001
	CN = Certification Authority Root Lleida SAS
	O = Lleida SAS
	2.5.4.97 = VATES- 9005710383
	SERIALNUMBER = 9005710383
	OU = Certification Authority Lleida SAS
	T = Subordinate Certificate Authority Lleida SAS

	L = BOGOTA
	C = CO

Valid from	It specifies the date and time from which the certificate is valid. It is synchronised with the UTC-5 time service.
Valid until	It specifies the date and time from which the certificate is no longer valid. It is synchronised with the UTC-5 time service.
Subject	See section "Rules for the interpretation of various forms of names".
Public key of the Subject	Encrypted in accordance with RFC 5280. The minimum key length is 1024 bits and RSA algorithm. The certificates issued by LLEIDA.NET have a length of 2048 bits and RSA algorithm.
Authority key identifier	It is used to identify the root certificate in the certification hierarchy. It normally references the "Subject Key Identifier" field of LLEIDA.NET as the digital certification authority.
Subject key identifier	It is used to identify a certificate containing a given public key.
Certificate policy	It describes the policies applicable to the certificate, specifies the OID and the URL where the certification policies are available.
Use of the key	It specifies the permitted uses of the key. It is a CRITICAL FIELD.
CCC distribution point	It is used to indicate the addresses where the LLEIDA.NET CRL is published. In the Root EC certificate, this attribute is not specified.
Access to the Authority's information	It is used to indicate the addresses where the LLEIDA.NET root certificate is located. Also, to indicate the address to access the OCSP service. In the LLEIDA.NET root certificate, this attribute is not specified.
Widespread uses of the key	Other purposes in addition to the use of the key are specified.
Basic restrictions	The extension "PathLenConstraint" indicates the number of sub-tiers that are allowed in the certificate path. There is no restriction for LLEIDA.NET so it is zero.

8.1.1 Version number

The certificates issued by the LLEIDA.NET Certification Authority comply with the X.509 Version 3 standard.

8.1.2 Certificate extensions

The X.509 version 3 extension of "certificatepolicies" is the object identifier of this CPS according to the Object Identifier section of the Certification Policy of this CPS. The extension is not considered as critical.

8.1.3 Object Identifiers (OIDs) of the algorithms

The object identifier of the signature algorithm can be:

- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption

- 1.2.840.113549.1.1.13 - sha512WithRSAEncryption

The object identifier of the public key algorithm is

1.2.840.113549.1.1.1 rsaEncryption

8.1.4 Name format

The guidance document that LLEIDA.NET uses for the unique identification of issued certificate holders is defined in the Distinguished Name (DN) structure of the ISO/IEC 9594 (X.500) standard.

Certificates issued by LLEIDA.NET contain the X.500 distinguished name (DN) of the issuer and recipient of the certificate in the issuer name and subject name fields respectively.

8.1.4.1 Root Certificate

The DN of the issuer name of the root certificate has the following fixed fields and values:

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

The following fields are included in the DN of the 'subject name':

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

8.1.4.2 Subordinated Debt Certificates

The DN of the issuer name of the certificates of LLEIDA.NET's subordinates has the following characteristics:

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

The following fields are included in the DN of the 'subject name':

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

8.1.4.3 Certificates of title

The DN of the issuer name of the LLEIDA.NET. holder certificates has the following general characteristics:

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

The description and fields in the DN of the subject name, for each type of certificate covered by this CPS, are detailed in document DOC-200216.2093009 - Certificate Profiles.pdf.

8.1.5 Restrictions on names

Names must be written in capital letters and without accents, the letter Ñ is only allowed for the names of natural or legal persons.

The country code is assigned according to ISO 3166-1 "Codes for the representation of country names and their subdivisions. Part 1: Country codes".

8.1.6 Certification Policy Object Identifier (OID)

The Certificate Policy object identifier is indicated in section 2.3 Document Name and Identification.

8.1.7 Use of the "Policy Constraints" extension

Not stipulated.

8.1.8 Syntax and semantics of policy qualifiers

The policy qualifier is defined in the "Certificate Policies" extension and contains a reference to the URL where the Certification Service Provider's CPS is published.

8.1.9 Semantic treatment for the "certificate policy" extension

Not stipulated.

8.2 CRL Profile

The CRLs issued by the LLEIDA.NET Certification Authority comply with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" and contain the following basic elements:

8.2.1 Version number

The CRL's issued by LLEIDA.NET comply with the X.509 version 2 standard.

8.2.2 CRL and extensions

Information on the reason for revocation of a certificate shall be included in the CRL, using the CRL extensions and more specifically in the revocation reasonCode field.

8.3 OCSP Profile

The OCSP service is compliant with RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

8.3.1 Version number

Compliant with OCSP Version 1 of RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

8.3.2 OCSP extensions

Not applicable.

9 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

LLEIDA.NET has passed annually since 2015 all the audits of its Information Management Security System that complies with the requirements of ISO/IEC 27001:2013 with the following scope described in the SoA and accessible in the accreditation certificate: https://www.lleida.net/docs/es/IS_632576_lleidanet.pdf

LLEIDA.NET has passed an Ethical Hacking audit to verify the resistance of its infrastructure to various potential security attacks.

LLEIDA.NET (parent company) obtained in 2018 the certification Trust Service Provider for Electronic Transactions according to the technical standard ETSI EN 319 401 V2.1.1. General Policy Requirements for Technical specifications Trust Service Providers (Article 44, Regulation (Eu) nº 910/2014) for its Qualified Electronic Certified Delivery Services and currently undergoes, with the periodicity indicated in EU Regulation 910/2014, audits of compliance with the requirements relating to qualified electronic trust service providers, for all the services it provides, on the basis of the standards:

- ETSI EN 319 401 V2.2.1 (2018-04) - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

The infrastructure and procedures of the certificate and time stamping service platform shall be assessed at least annually by a conformity assessment body.

The platform provider is accredited for compliance as a Trusted Service Provider, in application of EU Regulation No 910/2014 (eIDAS Regulation), ETSI EN 319 401 "General Policy Requirements for Trust Service Providers" and ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates":

The audit frequency is biennial (at least every two years), with annual follow-up audits.

Certificates that are considered qualified are subject to an annual audit that guarantees compliance with the requirements established in the European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates".

Information Security Management System according to the UNE-ISO/IEC 27001:2014 Standard:

Renewal every 3 years with annual follow-up audits.

Quality Management System in accordance with ISO 9001:2015:

Renewal every 3 years with annual follow-up audits.

Maturity of software lifecycle processes in accordance with ISO/IEC 33000 and ISO/IEC 12207, level 3 achieved:

Renewal every 3 years with annual follow-up audits.

9.1 Frequency of compliance checks for each entity

LLEIDA.NET carries out audits of its services and systems with the following frequency:

- ISO 27001, ISO 9001, ISO/IEC 33000, ISO/IEC 12207, annual periodicity
- eIDAS trust services, biannual basis

9.2 Auditor identification/qualifications

LLEIDANET entrusts its external audits to auditors with the necessary qualifications and accredited experience who act with complete independence and impartiality.

9.3 Relationship between the auditor and the auditee

The auditing companies have no connection with LLEIDANET and the professionals who carry out the audits are free of conflicts of interest.

9.4 Topics covered by the compliance check

In general, the objective of the audit is to establish that:

a) LLEIDA.NET guarantees the quality of the service provided.

b) LLEIDA.NET complies with the requirements of the Certification Policies and does so in the manner set out in its Statement of Business Practices.

c) LLEIDA.NET complies with its Certification Policies and Certification Practices Statement, approved by its Security Committee and with the provisions of current legislation.

d) LLEIDA.NET adequately manages the security of its information systems.

For this purpose, in general, the elements to be audited shall be the following:

- Processes and resources related to the lifecycle of certificates in both the Certification Authority and the Registration Authorities.
- Information systems.
- Security of the data processing centre.
- Documentación

9.5 Actions to be taken as a result of a deficiency

Depending on the severity of the deficiency, the actions to be taken may range from minor corrective actions communicated to the affected company personnel, to communicating the results to the safety committee for it to decide on a possible temporary cessation of activity.

9.6 Communication of results

The results of the audits are communicated to the LLEIDA.NET Security Committee so that it can take the appropriate action in accordance with the results.

The update of the positive results of the audits is available on the LLEIDA.NET website.

10 OTHER EMPRESARIALES AND LEGAL ISSUES

10.1 Tariffs

10.1.1 Fees for service activation

The rates not subject to commercial negotiation will be made public on the LLEIDA.NET website.

10.1.1.1 Fees for issuing or renewing certificates

The rates will be defined by LLEIDA.NET in accordance with the contracts entered into with its clients.

10.1.1.2 Certificate access fees

Access to the consultation of the status of issued certificates is free and free of charge and therefore no fee applies.

10.1.1.3 Fees for access to status information or revocation

There is no charge for requesting the revocation of a certificate. Access to the status information of issued certificates is free and free of charge and therefore no fee applies.

10.1.1.4 Fees for other services such as policy information

LLEIDANET will allow free access to the Certification Policies and the Certification Practices statement.

Additional services that have a cost and are not subject to commercial negotiation will have their rates published on the LLEIDA.NET website.

10.1.2 Refund policy

There is no general refund policy for the provision of these services. The value of the remaining term of the certificates will only be refunded in the event of termination of the ECD, if subscribers request it within two (2) months of the second publication of such termination and the transfer of the certificate to another ECD has not been executed at the request of the subscriber.

10.2 Financial capacity

LLEIDA.NET has sufficient assets to carry out its activities and, where appropriate, to meet its obligations.

10.2.1 Insurance coverage

LLEIDA.NET has Civil Liability Insurance appropriate to its activities, in accordance with the provisions of current state regulations.

10.2.2 Indemnification of third parties relying on the services provided by LLEIDANET

LLEIDA.NET has contracted a liability insurance for damages that may be caused by the use of the services provided by this ECD for the amount of detailing thus fulfilling the obligation set out in detailing.

10.3 Confidentiality policy

10.3.1 Confidential information

LLEIDANET considers confidential information to be all information that has not been classified as public.

The disclosure of this type of information is restricted to the cases provided for by law.

10.3.2 Information non-confidential

LLEIDA.NET considers information to be non-confidential:

- That contained in the Certification Practice Statement
- That contained in the different Certification Policies.
- All information that is classified as public

10.3.3 Responsibility to protect confidential information

LLEIDA.NET maintains security measures to protect all confidential information supplied to it directly or through the channels established for this purpose from its receipt until its storage and custody in the central archive where it will remain for the time indicated in the regulations in force. LLEIDA.NET has a security procedure for the handling and custody of information. Once the information provided by the applicant or holder has been received, a folder is created with the name, identification number and a file number is assigned. This data is related and registered for control and follow-up. This folder is assigned to the Approver, who always keeps it under code. Once the data and its authenticity have been verified by the Registration or Verification Entity, the folder is delivered to the Management Archive, which is responsible for storing it under code before being sent to the central archive together with the list of documents delivered. The central archive has environmental, logical and physical controls for the custody and conservation of this type of document. LLEIDA.NET has defined the positions and profiles that will have access to this information and the office of the Registration or Verification Entity has a security door and an alarm and monitoring system 7X24 hours throughout the year. Access to the information once filed must be supported by a request authorised by the Management of LLEIDA.NET. This allows us to ensure that the information of our holders will not be compromised or disclosed to third parties unless there is a formal request from a competent authority that requires it.

Persons who by reason of their work have access to confidential information must be aware of the security policies and must sign a Confidentiality Agreement. Likewise, personnel hired directly or indirectly and who participate in activities whose functions require knowledge of confidential information must sign the Confidentiality Agreement.

10.4 Personal data protection considerations

All data pertaining to natural persons are subject to the regulations on personal data protection. In accordance with law 1581 of 2012.

In accordance with the data protection legislation, personal data are considered to be any information relating to identified or identifiable natural persons.

Personal information that does not have to be included in the certificates and in the indicated mechanism for checking the status of the certificates is considered personal information of a private nature.

The following data are considered private information:

- Requests for activation of services, approved or denied, as well as all other personal information obtained for the issuance and maintenance of services, except for the information indicated in the corresponding section.
- Credentials generated and/or stored by the Certification Body
- Any other information that could be identified as "Confidential Information".

The data collected by the ECD will have the legal consideration that corresponds to its nature, normally being basic level data. Confidential information in accordance with data protection regulations is protected from loss, destruction, damage, falsification and unlawful or unauthorised processing.

10.4.1 Consent to use personal data

LLEIDA.NET informs that the personal data to which it has access in the framework of the provision of its services will be included in the register of processing activities for which it is responsible. LLEIDA.NET bases the processing of data primarily on: the legitimate interest it has in responding to requests for information about its services, the execution of a contract or the express consent of the data subject. Data subjects may withdraw this consent at any time.

The data collected are the minimum necessary for the provision of services and are kept for the periods established by law. They are not transferred to third parties, unless legally obliged to do so, nor are profiles created or automated decisions made based on this data.

LLEIDA.NET also informs you that, if you request the services covered by this CPS by telephone, your voice may be recorded during telephone conversations with the Registration Authority (RA) or the Digital Certification Authority (ECD), in order to allow secure processing of the request for the issuance or revocation of certificates. Prior to the recording, you will be provided with the basic data protection information stipulated in the data protection regulations and your express consent will be sought. The personal data collected in this way will be incorporated into the database file for which LLEIDA.NET is responsible.

For more information on exercising your rights under the regulations and on the processing of your personal data by LLEIDANET, please consult the more extensive legal notice, included at www.lleida.net/co.

10.4.2 Disclosure of personal data to third parties

Personal data may only be disclosed to third parties with the express consent of the data subject or if required by law.

10.5 Intellectual property rights

The reproduction, dissemination, public communication and transformation of any of the elements contained in this CPS, which are the exclusive property of LLEIDANET without its express authorisation, is prohibited.

10.6 Contractual and non-contractual liability

10.6.1 Limitation of liability

According to current legislation, LLEIDANET's liability does not extend to those cases in which the improper use of the certificate has its origin in conduct attributable to the Subject, and to the User Party for:

- Failure to provide adequate information, initially or subsequently as a result of changes in the circumstances reflected in the certificate, when its inaccuracy could not be detected by the certification service provider;
- Negligence with regard to the storage of signature creation data and its confidentiality;
- Not having requested the suspension or revocation of the certificate data in case of doubt about the maintenance of confidentiality;

- Having used the signature after the validity period of the certificate has expired;
- Exceed the limits stated in the digital certificate.
- In conduct attributable to the User Party if the User Party acts negligently, i.e. when it fails to check or take into account the restrictions in the certificate as to its possible uses and transaction amount limits; or when it fails to take into account the certificate's validity status
- Damage caused to the Subject or third parties that he trusts due to the inaccuracy of the data contained in the certificate, if these have been accredited by means of a public document, registered in a public register if this is required.
- Improper or fraudulent use of the certificate in the event that the Subject/Holder has assigned it or authorised its use in favour of a third party by virtue of a legal transaction such as a mandate or power of attorney, the Subject/Holder being solely responsible for the control of the keys associated with their certificate.

LLEIDANET shall not be liable in any case when faced with any of these circumstances:

- State of War, natural disasters or any other case of Force Majeure.
- For the use of certificates provided that it exceeds the provisions of the current regulations and the Certification Policies.
- For misuse or fraudulent use of certificates or CRLs issued by the CA
- For the use of the information contained in the Certificate or in the CRL.
- For the damage caused during the period of verification of the causes for revocation/suspension.
- For the content of digitally signed or encrypted messages or documents.
- For non-recovery of documents encrypted with the Subject's public key.
- In the event of theft or loss of credentials, and in those circumstances that make it necessary to proceed with the inactivation of the service.
- LLEIDANET does not guarantee the cryptographic algorithms and shall not be liable for damage caused by successful external attacks on the cryptographic algorithms used, if it has exercised due diligence in accordance with the current state of the art, and has proceeded in accordance with the provisions of this CPS and the applicable regulations.

10.6.2 Responsibilities of the ECD

LLEIDA.NET shall be liable in the event of non-compliance with its obligations as indicated in this CPS.

LLEIDA.NET is obliged, in accordance with current legislation and the provisions of the Certification Policies and this CPS, to:

1. Respect the provisions of current regulations, this CPS and the CP Certification Policies.

2. Publish this CPS and each of the Certification Policies on the website of . LLEIDA.NET WEBSITE..
3. Maintain the latest version of the CPS and the LLEIDA.NET Certification Policies published on the website.
4. Protect and safeguard your private key in a secure and responsible manner.
5. Issue certificates in accordance with the Certification Policies and the standards defined in this CPS.
6. Generate certificates consistent with the information provided by the applicant or holder.
7. Retain information on certificates issued in accordance with the regulations in force.
8. Issue certificates whose minimum content complies with the regulations in force for the different types of certificates.
9. Publish the status of issued certificates in a freely accessible repository.
10. Do not keep a copy of the applicant's or holder's private key.
11. Revoke certificates in accordance with the provisions of the Digital Certificate Revocation Policy.
12. Update and publish the list of revoked certificates CRL with the latest revoked certificates.
13. Notify the Applicant or Registrant of the revocation of the digital certificate within 24 hours of the revocation of the certificate in accordance with the digital certificate revocation policy.

10.6.3 Responsibilities of the Registration Authority

The Registration Authority shall assume full responsibility for the correct identification of applicants and the verification of their data, subject to the same limitations as set out for the ECD.

1. Being familiar with and comply with the provisions of this CPS and the Certification Policy corresponding to each type of certificate.
2. Custody and protection of your private key.
3. Verifying the identity of digital certificate Applicants and Holders.
4. Verifying the accuracy and authenticity of the information provided by the Applicant.
5. To file and keeping the documentation supplied by the applicant or holder for the period of time established by the legislation in force.
6. Respecting the provisions of the contracts signed between LLEIDANET and the holder.
7. Identifying and informing the CA of the causes for revocation provided by the applicants on the digital certificates in force.

   To notify LLEIDANET of any incident in the delegated activity.

10.6.4 Responsibilities of the subscriber of the services

The subscriber of the services shall assume all responsibility and risk for the reliability and security of the workstation, computer equipment or medium from which he/she uses the service.

1. Providing all the information required in the Digital Certificate Application Form to facilitate their timely and full identification.
2. Complying with the accepted and signed Digital Certificate Application Form.
3. Providing accurate and truthful information as required.
4. Informing during the validity of the digital certificate of any change in the data initially provided for the issuance of the certificate.
5. Responsibly safeguarding and protecting your private key.
6. Use the certificate in accordance with the Certification Policies established in this CPS for each of the certificate types.
7. As the holder, immediately requesting the revocation of its digital certificate when it becomes aware of a cause defined in the Circumstances for the revocation of a certificate section of this CPS.
8. Not to make use of the private key or the digital certificate once its validity has expired or it has been revoked.
9. Informing trusted third parties of the need to check the validity of the digital certificates they are using at any given time.
10. To inform the Third Party that trusts to verify the status of a certificate, the list of revoked certificates CRL, published periodically by LLEIDA NET, is available.
11. Not to monitor the provision of LLEIDA NET services, nor manipulate them or alter their correct operation, nor carry out acts of reverse engineering on their implementation.
12. Notifying any anomalous fact or situation relating to LLEIDA.NET's services and/or the evidence issued, and which may be considered as a cause for revocation of the same.

10.6.5 Responsibilities of the relying parties

Third Parties relying in their capacity as relying party on digital certificates issued by the LLEIDA.NET Certification Authority are under the obligation to:

1. To be familiar with the provisions on Digital Certification in the current regulations.
2. Being familiar with the provisions of the Certification Practice Statement.
3. Verifying the status of the certificates before carrying out operations with digital certificates.
4. Checking the CRL Revoked Certificate List before performing operations with digital certificates.
5. Knowing and accepting the conditions regarding guarantees, uses and responsibilities when carrying out operations with digital certificates.

10.6.6 Obligations of other participants

The Security Committee, as an internal body of the LLEIDA.NET Certification Body, is obliged to:

1. Reviewing the consistency of CPS with current regulations.
2. Authorising the required changes or modifications to the CPS.
3. Authorising the publication of the CPS on the LLEIDA.NET website.

4. Integrating the CPS with the CPS of third party certification service providers.
5. Approving changes or modifications to the LLEIDA.NET Security Policies.
6. Ensuring the integrity and availability of the information published on the LLEIDA.NET Certification Body website.
7. Ensuring the existence of controls over the technological infrastructure of the LLEIDA.NET Certification Body.
8. Requesting the revocation of a certificate if it has knowledge or suspicion of the compromise of the subscriber's private key or any other event that tends to misuse the private key of the certificate holder or the Certification Authority.
9. Being aware of and take appropriate action when security incidents occur.

10.6.7 Losses arising from the use of services and certificates

Except as provided by the provisions of this CPS, and as determined by law, LLEIDA.NET makes no other commitments or warranties, nor does it assume any other liability to certificate holders or third parties who rely on the services.

10.7 Indemnities

Revise section 10.2 Financial capacity

10.7.1 ECD indemnities

Revise section 10.2 Financial capacity

10.7.2 Compensation of subscribers

Revise section 10.2 Financial capacity

10.7.3 Indemnification of relying parties

Revise section 10.2 Financial capacity

10.8 Complaints. Complaints and jurisdiction

Requests, complaints, claims, requests and appeals regarding the services provided by Lleida SAS will be dealt with by various mechanisms available to the subscriber and will be resolved by relevant and impartial persons.

- By e-mail to clientes@lleida.net . You must attach the template available at www.lleida.net/co ECD_CO 4501 Template PQRSA Lleida SAS

- By telephone on +57 1 381 9903

Within a maximum period of 15 days they must be resolved and notified, after filing, analysis and drafting of a formal report that will be delivered to the subscriber.

LLEIDANET's activity is governed by Colombian law and by the Courts of Bogotá, unless the user is a consumer, which will result in the application of consumer protection regulations.

10.9 Period of validity of this document

10.9.1 Deadline

This CPS document and any amendments to it shall come into force upon publication on the LLEIDA.NET website and shall remain in force until superseded by a newer version.

10.9.2 Termination

This CPS document and any amendments shall remain in effect until modified or replaced by a newer version.

10.9.3 Effects of termination

Upon termination of this CPS and Policy, LLEIDA.NET participants are bound by its terms for all certificates issued for the remainder of the validity periods of such certificates. At a minimum, all liabilities related to the protection of confidential information will survive termination.

10.10 Individual notifications and communication with participants

Any notification concerning this CPS shall be made by e-mail or by registered mail addressed to any of the addresses referred to in the contact details section 2.8.2 contact

10.11 Amendments and changes

10.11.1 Procedure for making changes

Modifications to this document will be approved by the LLEIDA.NET Security Committee.

These modifications will be set out in a Certification Practice Statement Update document, the maintenance of which is guaranteed by LLEIDANET.

The updated versions of the Certification Practice Statement together with the list of modifications made can be consulted at www.lleidanet.es and more specifically at https://www.lleida.net/co.

LLEIDA.NET may modify the Certification Practices Statement by acting in accordance with the following procedure:

- The modification shall be technically, legally or commercially justified.
- All technical and legal implications of the new specification version must be considered.
- Change control shall be established to ensure that the resulting specifications meet the intended requirements that led to the change.

- The implications for users of the change in specifications shall be assessed in case the change needs to be communicated to them.

10.11.2 Modification mechanism and period

In the preparatory phase of the audits, LLEIDANET shall review this document to ensure that it remains up to date in relation to changes in the following aspects:

- Implementing legislation
- Operating guidelines issued by ONAC
- Publication of standards
- Improvements or non-conformities identified in audits
- Improvements made to services or launch of new services
- Adoption of third-party products and services that are integrated with those offered by LLLEIDANET.

LLEIDA.NET may make changes to this document without prior notice to users, such as, for example:

- Corrections of typographical errors in the document
- Changes in contact information.

LLEIDA.NET may make modifications to this document of which users will be informed, such as:

- Changes in service specifications or conditions.
- Modifications of URLs

Changes to this document are communicated to those bodies and third party companies issuing certificates under this CPS, as well as to the relevant auditors. In particular, ONAC shall be notified of changes to this CPS:

There will be a 15-day period in which interested parties may comment on the changes to the CPS and these comments, if any, will be taken into consideration in the final modifications to be approved by the Policy Approval body.

10.11.3 Circumstances under which an OID should be changed

Not stipulated.

10.12 Other provisions

10.12.1 Full Agreement

No stipulation.

10.12.2 Assignment

Issuing DCEs, subscribers, relying parties, Registration Entities or any other entity operating under this Certification Policy and Practice Statement are not entitled to assign any of their rights or obligations under this Certification Policy and Practice Statement without the prior written consent of LLEIDA.NET.

10.12.3 Severability

If any provision of this Certification Policy and Practices Statement is deemed invalid by a competent authority in the applicable jurisdiction, the remainder of the Certification Policy and Practices Statement shall remain valid and enforceable.

10.12.4 Enforcement (attorney's fees and duty exemption)

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

10.12.5 Force Majeure

LLEIDA.NET accepts no liability for any delay or failure to comply with an obligation under its CPS to the extent that such delay or failure is caused by events beyond its reasonable control.

10.13 Other Provisions

No stipulation.