Lleida.net eKYC

Statement of Identity Verification Service Provision Practices (IPSP)

Lleida.net
PCiTAL | Edifici H1 2a planta, B Â· 25003 Lleida (Spain)

Documentation Control

Description

The purpose of this document is to describe the compliance of the purpose and contents with ETSI EN 319 401 General Policy Requirements for Trust Service Providers and, in part, ETSI TS 119 461 Policy and security requirements for trust service components providing identity proofing.

Historical documentation

Version	Date	Author	Description
1	13/10/2022	Gloria Salvador	First Version

Document classification and status

Document classification	Public
Status	To be approved

Related documents

Description

Contents

0 Introduction

LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A. (Lleida.net) is a communications operator authorised by the Comisión Nacional de los Mercados y la Competencia to provide the following services: Data transmission - Internet access provider (10/12/1998); Fixed telephone service (11/05/2005); Data transmission - Storage and forwarding of messages (23/4/2008); and Mobile virtual operator -(5/12/2008). Furthermore, it is currently focused on the provision of trust services, providing security for the execution of legal acts on the Internet and their secure and registered remittance and notification.

For this purpose, the company is established as a Trust Electronic Services Provider under the name of Lleida.net.Lleida.net in accordance with the provisions of regulation EU 910/2014 (hereinafter, eIDAS Regulation) of the European Parliament and of the Council, of July 23, 2014, regarding electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / E.C. with effect from July 1, 2016.

The services provided cover Qualified and Unqualified Electronic Delivery, Advanced Electronic Signature and services that require the identification of end-customers.

The eIDAS regulation does not define identity verification as a trusted service per se. The identity verification service component is either part of the provision of Lleida.net's services as a Trusted Service Provider (TSP), or it can also be performed by a specialised Identity Verification Service Provider (IPSP) acting as a subcontractor of the TSP or other entities that need to identify their clients, for example, those subject to the AML Directives.

Should the task be used for issuing qualified or unqualified certificates for electronic signatures, whether owned or third party, full compliance with ETSI TS 119 461 is mandatory.

eKYC is Lleida.net's tool supporting the verification task according to this certification practice statement.

1 | Description of the services

The purpose of this document is to describe the compliance of the purpose and contents with ETSI EN 319 401 General Policy Requirements for Trust Service Providers and, in part, ETSI TS 119 461 Policy and security requirements for trust service components providing identity proofing of trust service subjects insofar as it defines an essential support line for identity verification within the framework of the eIDAS regulation, particularly but not exclusively for the issuance of certificates and their requirements according to Article 24.1 thereof.

Identity verification is the process of verifying an applicant's identity accurately to the required degree of certainty. Lleida.net has a remote identification tool, eKYC, which supports processes to verify the identity of third-party trust services and Know Your Customer (KYC) processes, e.g. for financial services.

With regard to eKYC and its procedures, Lleida.net, under the certification practices used in its services, provides a guarantee of reliability equivalent to that of physical presence. Compliance with eIDAS under the "High" assurance level allows Lleida.net to use these services for identity verification in its qualified and non-qualified services.

The provisions herein apply to all parties of Lleida.net services, including relying parties. All of them must be aware of the content of this document so they may establish their trust in the services provided by Lleida.net and adjust their actions to the provisions therein.

Third party organisations and independent authorities may also use this document to verify and certify that Lleida.net is acting under the policies and practices outlined in it.

Lleida.net uses this identity verification component to verify the identity of the following trusted services

1. Electronic registered delivery
2. Services relating to electronic registered delivery
    - Identification of senders and recipients
    - Record and electronic file documents
3. Advanced electronic signature

Furthermore, the features of eKYC and the process support provided by Lleida.net for third parties who need to identify their customers allow for customer identification to the required level.

1.1 Scope

This document sets out the general rules governing Lleida.net's rules and procedures for verifying the identity of its services. It also describes the practices to be implemented by third parties using eKYC for identity verification for their services.

Currently, the services covered do not include identifying persons for issuing qualified and unqualified certificates for electronic signatures.

This standard has been developed taking into account the following issues:

- It is based on ETSI EN 319 401, providing common requirements for all Trusted Service Providers (TSPs) implementing best practices for the use of selected media and applicable technologies that can be used to verify identity.
- It covers some of the security requirements of ETSI TS 119 461 covering the most common risks:
    - Impersonation: use of valid means of proof that do not correspond to the applicant but to another person.
    - Fake means of proof: use of forgeries with which the applicant wishes to obtain an identity which does not correspond to the real
    - one operational risks
    - and social engineering risks.
- Includes Video identification under the authorisation of the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC).

1.2 Scope of Application

Lleida.net services are offered subject to the version of this current document; this version will determine its validity and effects.

1.3 Document management, validity and advertising

1.3.1 Validity

Only the Policy Management Authority can approve Lleida.net Policies and Declarations of Practices. The Steering Committee performs this role.

Without prejudice to the provisions for modifying the Policies and declaration of practices and for a situation where Lleida.net ceases its activities, this document shall be valid for an indefinite period.

The invalidity of one or more of these policies' provisions and declaration of practices will not affect the rest of the document. In this case, said provisions will be considered not included.

1.3.2 Amendments

Only the Policy Management Authority may approve modifications to Lleida.net Policies and Declarations of Practices.

A change of version will be considered to exist when, at the discretion of the Policy Management Authority, the modifications may affect the acceptability of Lleida.net services. Otherwise, only the new wording of the same version will be considered.

1.3.3 Publication

Lleida.net Policies and declaration of practices will be published immediately after initially approved and, as applicable, upon modification. The web address (URL) for publication shall be:

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

1.3.4 Contact Details LLEIDANETWORKS

SERVEIS TELEMÀTICS, S.A. PCiTAL | Edifici H1

2ª planta, B

25003 Lleida (SPAIN)

info@lleida.net

(+34) 973 282 300

1.4 Terminology and abbreviations

Terms used for this Policy are defined as follows:

Applicant: person (natural or legal) whose identity is to be proven.

Client: third party that uses the Lleida.net service/tool to verify the identity of applicants.

reliable evidence: evidence that contains identifying attributes that are administered by an authoritative body

reliable source: any source, regardless of its form, trusted to provide data, information and/or evidence that can be used to prove identity

(Identity) attribute: quality or characteristic attributed to a person.

Reference LoIP: Level of identity verification (LoIP) that achieves a high level of trust based on compliance with best practice requirements for the identity verification process and considered suitable for trusted services policies as currently defined by ETSI standards.

linkage to the applicant: part of an identity proofing process that verifies that the applicant is the person identified by the evidence submitted

digital identity document: an identity document issued in a machine-processable form, which is digitally signed by the issuer, and which is in purely digital form

electronic identification means (eID): a tangible and/or intangible unit containing personal identification data and used for authentication of an online service

eID scheme: governance model and technical specifications that enable interoperability between the electronic identification media of different electronic identification providers.

(identity) evidence: information or documentation provided by the applicant or obtained from other sources relied upon to prove that the claimed identity attributes are correct.

False Acceptance Rate (FAR): The ratio of erroneously accepted verification transactions containing false biometric claims.

False Rejection Rate (FRR): Proportion of verification transactions with true biometric claims rejected in error.

identity: an attribute or set of attributes uniquely identifying a person within a given context.

identity document: physical or digital document issued by an authorised source and attesting to identity

identity verification context: external requirements impacting the identity verification process, as given by the purpose of the identity verification, the related regulatory requirements and the resulting constraints on the selection of attributes and evidence and on the identity verification process itself.

identity verification (process): a process whereby the identity of an applicant is verified through the use of evidence to prove the required attributes of identity

identity verification policy: a set of rules indicating the applicability of an identity verification service to a given community and/or class of application with common security requirements.

legitimate holder of the verification: person to whom the proof is issued.

Level of Identity Verification (LoIP): trust achieved in identity verification

liveness detection: measurement and analysis of anatomical features or voluntary or involuntary reactions to establish whether a biometric sample is being captured from a living subject at the capture site.

physical I.D. card: identity card issued in physical, human-readable form

physical presence: proof of identity where the applicant must be physically present at the location of the identity verification.

presentation attack: presentation to the biometric data capture subsystem to interfere with the operation of the biometric system.

Presentation Attack Detection (PAD) - automated determination of a presentation attack

proof of access: any source, regardless of its form, that can be relied upon to obtain reliable data, information and/or evidence that may be used in an identity verification process, provided that the applicant can prove access to the source

EXAMPLE:

Bank account, telephone number, email address or other resource owned by the applicant.

pseudonym: a fictitious identity that an individual takes on for a particular purpose, which differs from their original or true identity

remote identity verification: identity verification process where the applicant is physically away from the location of the identity verification.

subject: natural or legal person subscribing to a trust service

subscriber: natural or legal person bound by an agreement with a trust service provider to any obligation of the subscriber

additional evidence: evidence used in addition to authoritative evidence to strengthen the reliability of identity verification and/or as evidence of attributes that are not evidenced by authoritative evidence.

trusted registry: public registry, database, or another source that is trusted for the transmission of identity attributes in the context of identity verification

trusted service component: part of the overall service of a TSP.

validation: part of an identity verification process that determines if attributes are validated by the evidence provided and whether or not the evidence is genuine, reliable and valid.

The abbreviations used are

APCER Attack Presentation Classification Error Rate

BPCER Bona fide Presentation Classification Error Rate

eID electronic Identification

eMRTD electronic Machine Readable Travel Document

FAR False Acceptance Rate

FRR False Acceptance Rate

GDPR General Data Protection Regulation

ICAO Internation Civil Aviation Organization

IPSP Identity Proofing Service Provider

LEI Legal Entity Identifier

LoA Level of Assurance

LoIP Level of Identity Proofing

MRZ Machine Readable Zone

NCP Normalized Certificate Policy

PAD Presentation Attack Detection

QCP Qualified Certificate Policy

TLS Transport Layer Security

TSP Trust Service Provider

2. Lleida.net trust services general policies

2.1 Lleida.net Organization

2.1.1 Lleida.net Policies Administration Body

The Policy Administration Manager is a committee of Lleida.net who will approve these Policies and Declaration of Practices and any modifications. The Steering Committee performs this role. All Lleida.net policy documents and statements of practices must be approved by the Policy Management Body at least once a year, assessing the need to notify interested parties in each case.

The Policy Administration Manager is responsible for Lleida.net service provision matching these policies' provisions and declaration of practices and ensuring the proper execution of the established controls. Moreover, this person is responsible for the management, supervision and control of the provision of Lleida.net services and the properness of the provisions of this document.

The Policy Administration Manager is also responsible for analysing reports of full and partial audits of Lleida.net together with its services and for establishing and supervising, as applicable, any corrective actions to be taken.

The Policy Administration Manager will be appointed and dismissed by Lleida.net management by explicit resolution, of which there must be written proof.

2.2 Obligations

on the part of Lleida.net

Lleida.net assumes responsibility for ensuring that the services provided by Lleida.net are performed under the provisions of these Policies and Statements of Practice, as well as compliance with the requirements and controls set forth herein, along with any applicable legal provisions that may apply. In particular, it undertakes the following obligations:

1.-Provide services under the provisions of these Policies and Statements of Practice;

1. Ensure that the documentary evidence issued does not contain any erroneous or false information;

2. Use appropriate technologies and equipment with staff who are specifically trained and informed of their duties;

3. Provide uninterrupted access to its services, except in the event of scheduled interruptions or severe incidents or the event of unforeseen circumstances or force majeure;

4. Conduct reviews and audits as necessary to ensure compliance with applicable legislation, the Policies and Practice Statement and internal regulations;

5. Publish, on its website, information on the incidents that may have affected the services in such a way that it is possible to ascertain which, if any, documentary evidence has been affected.

On the part of clients/subscribers/applicants of Lleida.net services:

1. Use appropriate means when it comes to requesting services and, where appropriate, obtaining the resulting documentary evidence;

2. Know and accept the conditions and limitations on the use of documentary evidence as outlined in the relevant Policy;

3. Limit and adapt the use of the documentary evidence resulting from the service under the Policy that governs it.

4. Not to monitor the provision of Lleida.net services, nor to tamper with them or alter the correct functioning thereof, nor to reverse engineer the implementation thereof

5. Not to trust documentary evidence for uses other than those permitted in the relevant Policy.

6. To be aware of the provisions of these Policies, accepting and subjecting themselves to the provisions thereof and, in particular, to the responsibilities applicable to the acceptance and use of Lleida.net services and the documentary evidence resulting therefrom.

7. To notify any unusual event or situation concerning Lleida.net services and/or the documentary evidence issued, that could be grounds for the revocation thereof.

2.3 Responsibilities of Lleida.net

Lleida.net shall only be liable in the event of non-compliance with the obligations outlined in applicable legislation and these Policies and Statements of Practice.

Lleida.net shall not assume any responsibility for the use of the evidence issued for any use not authorised in these Policies and Statements of Practice.

Lleida.net is not responsible for the content of documents and data to which its services are applied and shall not be held liable for possible damages in transactions they have been used.

Lleida.net does not represent, in any way, the signatories, document generators or user parties of the documentary evidence it issues.

Lleida.net makes no warranties and assumes no liability to certificate holders or any other evidence issued or to the parties using them other than as outlined in these Policies and Statements of Practice.

Lleida.net has taken out a civil liability insurance policy with coverage of up to seven million euros (€7,000,000.00).

2.4 Personal data and confidentiality

2.4.1 Personal Data Protection

Lleida.net complies with the Data Protection Regulation (E.U. Regulation 2016/679, of April 27 2016) and Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights and its implementing regulations, guaranteeing Lleida.net's internal rules and procedures concerning the application of the level of security required by these regulations.

When providing a specific service, personal data must be collected from the signatory; it shall be verified that the signatory is informed and gives their consent to the processing of their data, to the purpose of such processing, and the inclusion thereof in the file set aside for this purpose by Lleida.net.

Personal data shall not be disclosed to third parties without the express consent of the data subject, except where expressly authorised by law.

2.4.2 Confidential information

Any information that Lleida.net does not expressly declare public shall be deemed confidential. The private keys used by Lleida.net and its administrators and operators.

- Information concerning the operations carried out by Lleida.net.
- Information on security, control and audit procedures.
- The personal information of the signatories

Public information and, therefore, accessible by third parties shall be considered the information contained in these Policies and Statements of Practice and any other declared by Lleida.net.

2.4.3 Duty of secrecy

All persons with an employment or professional relationship with Lleida.net are obliged to maintain the utmost confidentiality vis-à-vis the confidential information to which they have access under this relationship. Lleida.net will inform them in writing, at least at the commencement of the relationship, keeping a record that said the recipient has received information. This obligation shall remain in force once the relationship with Lleida.net has come to an end.

2.5 Audits

Lleida.net will conduct functional audits of Lleida.net. An independent auditor must conduct the audits. Audits of the trust services shall also be conducted every two years.

All audits shall verify, as a minimum, that Lleida.net's practices comply with the provisions of these Policies, with the provisions of the administrative authorities as well as with regulations currently in force, and that they have a methodology in place to ensure the quality of the services provided.

2.6 Rates

Lleida.net shall publish the rates it charges for providing each of its services on the website.

Lleida.net shall not charge a fee for access to the information required to verify the validity of documentary evidence issued, nor to these Policies and Statements of Practice, nor to information required by these Policies and Statements of Practice to be made public

2.7 Complaints and Jurisdiction

2.7.1 Communication of complaints

If a User Party has a complaint about Lleida.net services, they should report it to Lleida.net by any of the contact channels indicated in section 1.3.4 herein. Lleida.net shall reply to the complaint within one week at the latest. Lleida.net shall reply to the complaint within one week at the latest.

2.7.2 Jurisdiction

The users of Lleida.net services accept the jurisdiction of the courts and tribunals of Lleida about any dispute that may arise vis-à-vis the provision of services by Lleida.net, expressly waiving any other jurisdiction that may correspond thereto. International treaties and convention provisions shall apply if the user is considered a consumer. The amicable resolution of disputes shall always be sought.

3. Policy and basic statement of practice vis-à-vis the provision of the identity validation service

This Policy governs the provision of the validation service by Lleida.net Entities availing of the eKYC tool to identify their customers shall do so under the principles set forth herein and the information provided by Lleida.net.

3.1 Basic statement of the identity validation service

The Lleida.net Basic Identity Proofing Service Practice Statement (IPSP) sets out the core terms and conditions of the service, which, together with more specific terms and conditions, are set out herein. Accordingly, by way of this basic statement, Lleida.net hereby states that:

Ownership

IPSP is a component of the LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A., whose contact details are indicated in section 1.3.4 herein

Service availability

Service availability shall be as set out herein.

Publication of the Policy

Users shall have access to this Policy or the version applicable at any given time at: https://www.lleida.net/es/politicas-y-practicas

Cryptographic Mechanisms

The electronic signature of the identity validation certificates is carried out by calculating the hash using SHA256, and based on X.509 version 3 certificates and RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", using qualified certificates issued by InDenova or Firmaprofesional as a backup provider.

Validity of identity validation certificates

IPSP does not establish any other limitations to the trustworthiness of this service component beyond those inherent in the technologies used and legal presumptions. Lleida.net will always make use of the most advanced cryptographic techniques.

Applicability

Lleida.net deems that the most appropriate use of the identity validation service component is to obtain documentary evidence of the identification of the parties using its services. Furthermore, obtaining evidence of identification of user parties from services of the same nature provided by other trust service providers, provided that the issuance of certificates (qualified and unqualified) for electronic signatures is excluded. It can also be used to obtain evidence of customer identification in Know Your Customer (KYC) processes, e.g., by parties subject to the AML Directives, particularly those obliged to comply with SEPBLAC authorisation in video identification processes.

Obligations

The relying parties' obligations are described in this document.

Operations Record-keeping

Lleida.net records its transactions and saves this information under adequate security conditions

Regulations

The provision of the identity validation service by Lleida.net is carried out under the applicable Spanish and European legislation, with these Policies and Statements of Practice, as well as with Lleida.net's internal regulations.

Responsibility

Lleida.net's responsibilities and limitations are set out above herein.

Complaints

All complaints from users and third parties regarding the validation of identity shall be reported per the provisions set forth herein. Should the parties fail to reach an agreement, they shall submit to the courts and tribunals indicated in the "Jurisdiction" section.

Guarantee and Audits

Lleida.net now ensures that identity verification is carried out under the provisions outlined in this Policy and Statement of Practice. In this regard, Lleida.net shall conduct frequent audits of Lleida.net's functioning under the guidelines set forth herein.

Rates

Lleida.net may charge a fee for providing identity validation services under the rates published on its website at any given time.

Providers

Lleida.net uses the services of providers intending to issue documentary evidence of identity validation, namely the following:

- Firmaprofesional, s.a.
- Indenova, s.l.u.

3.2 Community of users

The community of users for identity validation are the users of Lleida.net services or third parties who can prove a legitimate interest in validating their users. The people and entities that trust the certifications issued by Lleida.net are also part of the community.

Also part of the community is the people and entities that use the certificates issued by Lleida.net Lleida.net shall be responsible for validating the service user's identity for its services. It shall also be responsible for generating and issuing signed certificates that record the documentary evidence, the validation result, and the time they were generated.

User parties are those who request Lleida.net users of its services to make use of the identity validation component. User parties are those who request Lleida.net users of its services to make use of the identity validation component. Furthermore, those who count on the certifications of the validation results generated by Lleida.net.

All of them are subject to the provisions of this Policy.

3.3 Uses of identity validation

Lleida.net deems that the most appropriate use of the identity validation service component is to obtain documentary evidence of the identification of the parties using its services. Furthermore, to obtain proof of identification of user parties from services of the same nature provided by other trust service providers, provided that the issuance of certificates (qualified and unqualified) for electronic signatures is excluded. It can also be used to obtain evidence of customer identification in Know Your Customer (KYC) processes, e.g., by parties subject to the AML Directives, particularly those obliged to comply with SEPBLAC authorisation in video identification processes.

3.4 Obligations

As well as the obligations set forth by law and the aforementioned ones, the following specific obligations are set out vis-à-vis the performance of tasks and provision of identity validation tools.

Lleida.net

1. Follow the identity validation procedure in the manner set forth herein and report the same, issuing the corresponding certificate.
2. Provide appropriate resources for the subjects of identity validation to access the tool and follow the procedure
3. Receive and store the documentation for identity validation, generating the identity validation certificate on the basis thereof and making it available to the applicant.
4. Use appropriate electronic signature and time stamp resources to generate certificates.
5. Ensure the confidentiality of validation processes, using encryption techniques where applicable.

User parties (customers, applicants and subscribers)

1. Ensure that identity checks are based on a legal relationship with applicants and are not carried out for spurious reasons.
2. Provide Lleida.net with reliable and up-to-date contact details of the subjects.
3. When the user is using eKYC to perform identification, follow the guidelines in the Lleida.net documentation for the level of identification required and the information contained herein
4. Applicants must submit authentic and valid documents, follow Lleida.net's instructions during the identity validation process, and abstain from using physical or technical resources that alter or hinder the ability to obtain the images required for the validation.

5. Notify any out-of-the-ordinary event or situation concerning identity validation or the certificates issued, which could result in the loss of reliability.

Providers

1. Ensure that digital signature services for identity validation certificates are qualified under the eIDAS regulation.
2. Ensure that time-stamping services used for identity validation certificates are deemed as qualified under the eIDAS regulation
3. Provide Lleida.net with the digital certificates necessary for the electronic signing and time-stamping of the documentation issued by Lleida.net as part of the identity validation process.
4. Provide Lleida.net with the time-stamping service for the identity validation process.
5. The services above may be provided internally by Lleida.net once it expands the functionality of its trusted services infrastructure.

3.5 Record of information concerning identity validation

Lleida.net keeps records of all relevant information concerning its operations for 15 years are protected to ensure the integrity and confidentiality thereof.

The records can be accessed by those with a legitimate interest in accessing them and by the authorities and courts that so require them by the provisions of the law.

In particular, records, including the time at which they were generated, are kept on the following events:

- Image capture of the subject of the identity validation process.
- Identity documents are shown as part of the process;
- Video of the identification process

The procedures for generating and retaining these records are set out in IPSP's internal management documentation.

3.6 Identity verification

3.6.1 Description of the process

Under ETSI TS 119 461, the identity validation process is usually split into five tasks:

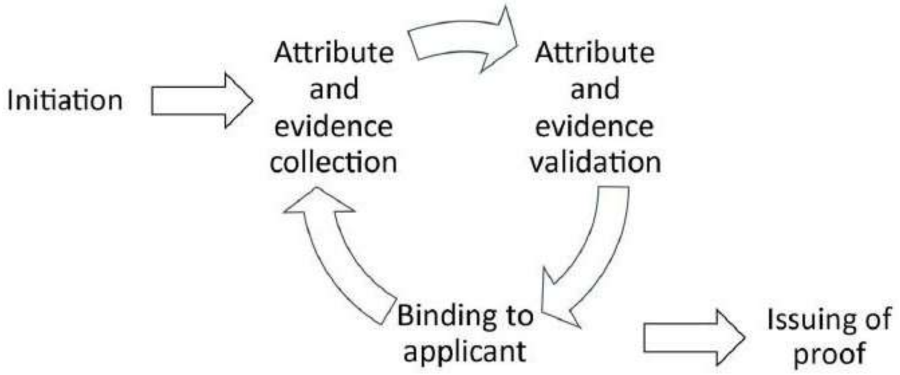
1) Initiation.

2) Attribute and evidence collection.

3) Validation of attributes and documentary evidence

4) Correlation with the applicant.

5) Issuance of the identity test result.


Initiation
Attribute and evidence collection
Attribute and evidence validation
Binding to applicant
Issuing of proof

The identity validation process gets underway by showing certain information to the applicant and obtaining their consent concerning the remote identification process. The applicant must follow the process instructions in which images shall be captured of the person and of the identity documents they show in a certain context. The extracted information shall be validated and reviewed manually or automatically.

3.6.2 Availability of the service

The identity validation component is available continuously, except for scheduled maintenance, outages due to third-party services, unforeseen circumstances and force majeure, in which case the interruption shall not exceed 48 hours.

3.6.3 Identity verification stages

1) Initiation.

Before getting the identification process underway, eKYC shows the information on the documentary evidence to be collected as part of the identity validation process

Information is provided on alternative identity validation mechanisms, and the applicant's consent is obtained.

Furthermore, an OTP can be configured and sent to complete the process. The OTP can be received by email, SMS or both.

2) Attribute and evidence collection.

eKYC may collect different context-dependent attributes defined by the customer or by Lleida.net

The fields that can be requested, saved or verified are listed in the following documentation

https://api.lleida.net/eKYC/docs/v4/en/#verify

In all contexts, a minimum set of data is collected that identifies the applicant and that, in the case of natural persons, includes as a minimum:

- Name and surname

- identification number

The following documentary evidence is captured during the process:

a) Photograph of the front of the identity document taken during the video identification.

b) Photograph the reverse side of the identity document taken during the video identification.

c) Photograph of the applicant taken during the video identification.

d) Session start date and time.

e) Session end date and time.

f) Result of the validation (positive or negative, assisted or automatic).

g) Geolocation of the interested party via the device used and user authorisation (optional).

h) Technical details of the document validation.

i) Video of the identification process.

3) Validation of attributes and documentary evidence

eKYC performs identity validation by capturing images of physical documents shown by the applicant. The tool supports different identification documents (passports, national documents, driving licenses) issued by different countries worldwide

The applicant must submit the physical document during the identity validation process. In the process, photos of the front and rear of the identity document are made, and a recording of the process is made.

The integrity of different security elements is validated, such as the coherence of dates and the information in the MRZ zone is matched with the information in other parts of the document shown.

The photograph of the document is compared to the photographs taken while capturing the documentary evidence.

All collected elements are automatically analysed, and an analysis result is provided based on thresholds for the defined identity validation context. Depending thereon, the following validations may be performed:

- Fully automatic, which ends when the aforementioned automatic analysis has been completed, and the result can be positive or negative.
- Manual approval. An agent shall review the evidence and the validation outcome, decide whether the validation was positive or negative, and may record the reason for the decision reached.
- Mixed: An agent may review the documentary evidence if the automatic validation gives a negative result

Registration agents receive tool-specific training on data protection and the characteristics of the documents and are granted access to information sources such as PRADO to ascertain the physical characteristics of the documents to identify fake documents. Lleida.net shall be responsible for delivering this training when acting as an IPSP and with its client when using the eKYC tool to verify the identity of applicants

In some contexts, agents can consult trustworthy sources, such as RENIEC in Peru, to validate the document's status.

4) Correlation with the applicant.

eKYC compares the applicant's photo with the photo on the submitted ID document.

Depending on the context, a similarity threshold between the two pieces of documentary evidence is established to rate the identification as positive. Depending on the context, a similarity threshold between the two pieces of documentary evidence is established to rate the identification as positive.

The validation process is recorded, and proof of life is conducted during the validation process to ensure that the applicant is a real person and not a still image.

Depending on the context and the documentary evidence of life, the applicant may be asked to perform gestures or movements randomly selected from a list of possible actions. These contexts are intended to make the process more secure by making it impossible to pre-record videos

5) Issuance of the result of identity validation

Lleida.net issues a document containing all the information of the identity validation process, which is electronically signed with a qualified certificate and time-stamped with a qualified service for this purpose.

In certain identity validation contexts, high levels of authentication can be supported and ensure that the conditions for compliance with SEPBLAC's remote identification authorisation are met.

Documentary evidence shall be stored for 15 years.

3.7 Security measures

Lleida.net has implemented an information security management system certified using the ISO / IEC 27001 standard that reaches the trust services that are the object of this Policy.

For this purpose, Lleida.net has documented, adopted and implemented, following a risk analysis, a security policy as well as the necessary security controls to mitigate the risk identified in the following areas:

1. Adoption of a security policy, including management guidelines on information security, the set of policies for information security, and the revision thereof.

2. Implementing controls on organisational aspects of information security, allocating responsibilities for security, segregation of duties, information security in project management and implementation of mobility controls. Information security awareness, education and training.

3. Implementation of processes for asset management, implementing an inventory of assets with recommendations on acceptable use thereof based on the classification of the information processed or stored

4. Implementation of hardware and software access control management processes, access control to networks and associated services, user access management, user registration/de-registration management, management of access rights assigned to users, and management of access rights with special privileges.

5. Management of sensitive user authentication information, review, withdrawal or adaptation of user access rights, and the use of sensitive information for authentication.

6. Control of access to systems and applications, with controls in place to restrict access to information, secure login procedures, user password management, use of system administration tools and control of access to source code.

7. Implementation of physical and environmental security measures, establishing a physical security perimeter, physical entry controls, security of offices, offices and resources, as well as protection ag

8. Equipment security control measures, implementation of site controls and equipment protection, supply installations, cabling security, equipment maintenance, off-site asset egress procedures and off-site equipment and asset security.

9. Establishment of responsibilities, documentation and procedures, change management, capacity management, separation of development environments, testing and production, and protection against malware.
10. Backup policies, activity logging and monitoring, logging and managing activity events.
11. Technical vulnerability management, information security incident and improvement management, security incident response, and information security continuity planning.

The procedures above are set out in the internal management documentation of the confidential eKYC tool.

4. Termination

Should Lleida.net cease to operate the services set forth herein, it shall notify the relevant Supervisory Authority. This certification body has performed its most recent conformity assessment, as well as all of its current and former customers within the last five years, at least forty-five (45) calendar days before the termination of the service.

Within the notification period, customers may request access, at their own expense, to the documentary evidence generated in their interactions with Lleida.net, which shall endeavour to provide them in a human-readable format. In any case, and for the appropriate legal intents and purposes, Lleida.net shall store the documentary evidence in PDF format under the internal procedures on generating and storing documentary evidence in force as of the expiry of the notification period

Due to the nature of the generated documentary evidence itself and the fact that it is sent to customers and the maintenance of the public key used to sign documentary evidence by the digital signature provider, the transfer of the rights and obligations of the service to a third-party shall not be required if Lleida.net ceases to exist a legal entity.

The actions to be carried out vis-à-vis dissolving the legal entity that is Lleida.net shall be as follows:

- Notify current customers and people who have been customers within the last five years at least forty-five (45) calendar days before the service ends.
- Notify service providers.

- Notify the Ministry of Industry.
- Delete the private key used to sign the documentary evidence.