Lleida.net

POLICY AND PRACTICES STATEMENT ADVANCED ELECTRONIC SIGNATURE and REGISTERED ELECTRONIC COMMUNICATIONS ATTESTATION CERTIFICATION SERVICES

AES-RECA-PPS 01.00.00|

Version 2.0

3 January 2022

LLEIDA.NET
PCiTAL · Edificio H1, 2a planta B, 25003 Lleida (SPAIN)

Documentation Control

Description

This document and its provisions specify the Policy and practices of Lleida Networks Serveis Telematics for its advanced electronics signature services and the technical aspects of the registered delivery service. Regarding its purpose and content, this Policy is governed by the provisions of Article 26 and 43 of the eIDAS Regulation (UE 910/2014); the Technical Standard defined in ETSI EN 319 401 "General policy requirements for trusted service providers", and ISO/IEC 29115:2013 "Information Technology - Security Techniques - Entity Authentication Guarantee Framework", and other regulations of specific jurisdictions in the Supplements to this Policy

The guidelines on electronic identification resulting from Commission Implementing Regulation (EU) 2015/1502 as of 8 September 2015 laying down security levels for electronic identification means by Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market are taken into account.

Furthermore, Resolution ETD/465/2021, dated 6 May, which regulates the methods of remote video identification for the issuance of qualified electronic certificates, is also considered.

Document history

Version	Date	Author	Description
1	2019-10-31	MG, IM, JR, EP, ES	AES + ERDS
2	2022-01-03	BP	Compliance with the new Law 6/2020, governing some aspects of eTrust services.

Clasificación y estado del documento

Document classification	
Status	

Related documents

Description

Overview

1 INTRODUCTION

LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A. (hereinafter Lleida.net or LLEIDA.NET) is a telecommunications operator authorised by the Spanish authorities and a qualified trust service provider operating by the provisions of European Regulation (EU) 910/2014 (known as the eIDAS Regulation). It offers trust-related services all over the world.

LLEIDA.NET was authorised for different telecommunication services in its development:

- • Telecommunications Market Commission for the provision of data transfer- Internet access provider services (10/12/1998);
- • Fixed telephony services (11/05/2005); Data transfer - Message storage and resending (23/4/2008); and
- • Virtual - Full mobile operator (5/12/2008),

Nowadays, it provides several electronic evidence services as a Trust Services Provider to guarantee the probative value of legal digital documents on the Internet and qualified registered delivery, registered mail, registered SMS and other registered communication services.

To this end, the Company acts as a qualified trust service provider operating under the name "Lleida.net Prestador de Servicios de Confianza" (from now on, LLEIDA. NETPSC) by the provisions of Law 6/2020, of 11 November, regulating certain aspects of qualified electronic trust services (TSL), and Regulation (EU) 910/2014 (hereinafter, eIDAS Regulation) of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Furthermore, Resolution ETD/465/2021, dated 6 May, regulates remote video identification methods for issuing qualified electronic certificates, is also considered.

The structure and contents of this Policy have been defined as per ETSI Technical Standard EN 319 401– “General Policy Requirements for Trust Service Providers”; ISO/IEC 29115:2013 “Information Technology - Security Techniques - Entity Authentication Guarantee Framework”, and other regulations of specific jurisdictions in the Supplements to this Policy

It also takes into account electronic identification guidelines derived from Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means under Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions.

1.1 Overview

This Policy describes:

- Participants and their roles
- How the Signatory Identification and the Declared Identity are verified in each of the services and their different modalities.
- How the Signature is created binding the signatory with the signed document.
- Facilities management (physical security, personnel, audits, etc.).
- Audit procedures
- Legal and Business matters.

Lleida.net will issue Attestation Certificates for Advanced Electronic Signatures Services (including Electronic Consent for Contract Formation) and for Registered Electronic Communications.

This Policy and Practices Statement Document identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon, and management of Electronic Signature Credentials and Registered Electronic Communications Attestation Certificates The provisions of this document about practices, level of services, responsibilities and liability bind all parties involved including Lleida.net, its appointed RAs (Registration Authorities), Subscribers and Relying Parties. Specific provisions might also apply to other entities such as certification service providers, application providers, etc.

This Policy and Practices Statement Document describes the requirements to issue, manage and use Electronic Signature Credentials and Electronic Communications Attestation Certificates issued by Lleida.net.

A subscriber or relying party of a Lleida.net Electronic Signature Service or Registered Electronic Communications Attestation Certificate must refer to the Lleida.net Policy and Practices Statement to establish Trust.

1.2 Document name and identification

According to the eIDAS Regulations, and within the scope of this Advanced Electronic Signature and Registered Electronic Attestation Service Policy and Practice Statement, the services offered by LLEIDA.NET are defined as:

Table 1 Policy OID

Name	Policy OID
Electronic Signature/Seal & Electronic Contract Offer and Confirmation	
Signature	1.3.6.1.4.1.52376.2.5.0
Seal	1.3.6.1.4.1.52376.2.5.1
Simple Signature	1.3.6.1.4.1.52376.2.5.0.0
Advanced signature -no certificate	1.3.6.1.4.1.52376.2.5.0.1
Advanced signature -with certificate	1.3.6.1.4.1.52376.2.5.0.2
Simple Seal	1.3.6.1.4.1.52376.2.5.1.0
Advanced seal -no certificate	1.3.6.1.4.1.52376.2.5.1.1
Advanced seal -with certificate	1.3.6.1.4.1.52376.2.5.1.2
Advanced signature- non qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.0
Advanced signature- qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.1
Advanced seal- non qualified certificate	1.3.6.1.4.1.52376.2.5.1.2.0
Advanced seal- qualified certificate	1.3.6.1.4.1.52376.2.5.1.2.1
Advanced signature- qualified certificate-nonqualified device	1.3.6.1.4.1.52376.2.5.0.2.1.0
Advanced signature-qualified certificate-qualified device	1.3.6.1.4.1.52376.2.5.0.2.1.1
Advanced seal- qualified certificate-nonqualified device	1.3.6.1.4.1.52376.2.5.1.2.1.0
Advanced seal-qualified certificate-qualified device	1.3.6.1.4.1.52376.2.5.1.2.1.1
Advanced signature on server -non qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.0.1
Advanced signature on server- with qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.1.1
Advanced signature on server- with qualified certificate-nonqualified device	1.3.6.1.4.1.52376.2.5.0.2.1.0.1
Advanced signature on server- with certificate -qualified device	1.3.6.1.4.1.52376.2.5.0.2.1.1.1
Electronic Delivery	
Electronic comunication atesttations	1.3.6.1.4.1.52376.2.4.0
Registered email	1.3.6.1.4.1.52376.2.4.1
Registered electronic delivery (non email)	1.3.6.1.4.1.52376.2.4.2
Registered email	1.3.6.1.4.1.52376.2.4.1.0
Qualified registered email	1.3.6.1.4.1.52376.2.4.1.1
Registered electronic delivery (non email)	1.3.6.1.4.1.52376.2.4.2.0
Qualified registered electronic delivery (non email)	1.3.6.1.4.1.52376.2.4.2.1

This Policy and Practice Statement is available at https://lleida.net/policies.

1.3 Intervening roles and entities

This Policy sets the general rules and practices for the provision of Advanced Electronic Signature and Registered Electronic Communication Attestation services by Lleida.net. These general rules and practices apply to all persons and entities intervening in these Services, including parties being users of the services and relying parties.

All intervening parties must know the contents of this document to understand how evidence and Attestation are managed and the mechanisms that preserve Trust in advanced electronic signatures and electronic contact consent attestation as delivered by LLEIDA.NET Services.

Third parties can also use this document and independent entities to check, verify and certify that Lleida.net performs as per this Policy and Practices Statement.

This document becomes effective and binding for signatories and originators (natural persons) by accepting any contract or signature request and proceeding with the signature journey. For contracting entities and originators (legal persons), there are specific “Terms and Conditions” relevant, among other issues, in signatory identification and Electronic Communication addressee identification.

For relying parties, this document becomes binding by merely addressing a Lleida.net issued document signature verification request. The subscriber agreement forfeits the consent of the relying party about accepting the conditions laid out in this document

1.3.1 Identity Validator or Registration Authority

The identity validator performs the same functions as a Registration Authority (RA) in a certificate issuing service framework. Therefore, since it is a term coined in the Trust Services sector, the identity verifier will be named in this document as Registration Authority or RA.

LLEIDA.NET as a trust service provider can offer its Advanced Electronic Signature and Electronic Registered Communication service, directly, using its own Registration Authority (RA) service, to validate the identity declared by the signatory or addressee; or in some cases, the identity validation can be carried out by the entity that offers the contract or document to be signed through the Advanced Electronic Signature service, or dispatches a Registered Electronic Communication. In both cases, the term RA defines the roles and procedures to identify the signatory or addressee correctly.

In other words, the RA functions can be performed by the entity that offers the signatory the document to be signed through LLEIDA.NET Advanced Electronic Signature service or dispatches a Registered Electronic Communication. This entity can be named Offeror or Originator.

In the case of financial institutions, and other entities complying with AML-TP (Anti-Money Laundering and Terrorism Prevention) regulation, LLEIDA.NET understands that they will proceed according to Due Diligence practices and KYC ("Know Your Customer") procedures to identify and verify the identity of their customers.

The conformity assessment body Trust Conformity Assessment Body S.L.U.

(TCAB) has assessed the Remote Advanced Electronic Signature Service provided by Lleidanetworks Serveis Telemàtics SA by the applicable regulations and technical standards and has verified that the service provided complies with Article 26 of the EIDAS Regulation (Regulation (EU) No 910/2014).

The accreditation proves that the Remote Advanced Electronic Signature service, provided by Lleidanetworks Serveis Telemàtics SA, complies with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 403 v2.2.2.2 and the Commission Implementing Regulation (EU) 2015/1502.

Likewise, the Trust Conformity Assessment Body S.L.U. (TCAB) TCAB) has assessed the Remote Identification Service provided by Lleidanetworks Serveis Telemàtics SA by the applicable regulations and technical standards and has verified that the service provided complies with the requirements and standards established by Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) and met all the relevant requirements defined in the standards and regulation: EU Commission Implementing Regulation 2015/1502, ETSI EN 319401, ETSI 319 411-1, National Law 10/2010, Royal Decree 304/2014 and Spanish video-identification authorisation published by SEPBLAC. Entities acting as RAs are bound by this Policy and Practices Statement, together with a formal contractual relationship with Lleida.net.

Any RA is subject but not limited to the following obligations:

- • Identification and authentication of Signatories and Originators
- • Establishment of a contractual relationship with Signatories or the entities those signatories represent and with Originators of the entities those Originators represent
- • Initiate the advanced electronic signature procedure once the signatory's identity has been validated, using the electronic means offered by the LLEIDA.NET Advanced Electronic Signature service.
- • Initiate the Registered Electronic Communication once the identity of the Originator has been validated, using the electronic means offered by the LLEIDA.NET Registered Electronic Communication Attestation service.
- • Recording, maintaining, archiving and custody of any relevant signatory and originator identity-related documentation as long as the AML-TP regulation mandates it.

•

- Comply with applicable Personal Data Protection Regulations.
- • Provide any information required by Lleida.net, about identity validation procedures, at any time, and especially during the annual Policy and Practices Statement compliance evaluation
- • Authorize Lleida.net to perform and conduct Electronic Deliveries and Electronic Records generation and keeping on behalf of the RA and represent the RA for such Electronic Deliveries and Electronic Records generation and custody.

According to Trust Services regulations, identity validation related documents shall be archived for 15 years, except those cases where applicable local regulations could mandate a different term.

RAs acting in Lleida.net Advanced Electronic Signature and Registered Electronic Communication Attestation Service are obliged to comply with this Policy and Practices Statement and successfully pass any Policy and Practices Statement compliance assessment to be performed by Lleida.net or by any other conformity assessment body designated by Lleida.net.

1.3.2 Digital Witness & Electronic Communication Attestation Provider:

Role played by LLEIDA.NET as a trusted third-party attests the participants in a document or content communication, signature and the content of signed documents, and other electronic evidence. The attestation includes relevant information such as IP addresses, email addresses, mobile phone numbers, geolocation, and date, and evidence that the underlying procedures meet the requirements defined in Articles 26 and 43 of the eIDAS Regulation (EU) or other relevant country-specific requirements

1.3.3 Offeror or Originator Entity

The entity that offers the contract or document to be signed through the LLEIDA.NET Advanced Electronic Signature service, or that dispatches an Electronic Communication to be attested by Lleida.net Registered Electronic Communication Attestation service. In some cases, the same entity can also perform RA functions identifying the signatory or addressee before contract signing or electronic communication delivery procedure.

1.3.4 Signatory

Natural person who signs a document through the LLEIDA.NET Advanced Electronic Signature service. It is generally the person who expresses consent for the clauses of a document and completes the contract offered by the Originator.

1.3.5 Recipient

Natural or Legal person to whom a Registered Electronic Communication is dispatched through Lleida.net Registered Electronic Communication Attestation service. It is usually identified by the Originator by an email address, a mobile phone number, or a Digital Certificate signs a document through the LLEIDA.NET Advanced Electronic Signature service

1.3.6 Relying Party

Person or entity who understand and accepts a Lleida.net Attestation as proof of a contract formation, a document signature, or a Registered Electronic Delivery, through its Advanced Electronic Signature service or its Registered Electronic Delivery Attestation service.

The relying parties should know and abide by the warranties, limits and responsibilities defined in this Policy.

1.3.7 RA Verification Authority

Role played by Lleida.net when verifying the Identity of an RA, Registering the RA, and providing the RA with Credentials for performing as an RA.

This Role can be delegated to a Delegated RA Verification Authority.

1.3.8 Delegated RA Verification Authority

Role played by some Lleida.net Business Partners, allowing them to perform, on behalf of Lleida.net, RA Verification Authority functions.

This role cannot be delegated, outsourced or subcontracted, and is subject to specific Contractual Terms and Conditions set between Lleida.net and its Business Partner.

1.4 Policies Administration

The Policy Management Authority of Lleida.net manages this Policy and Practices Statement. Lleida.net registers, observes the adherence to its procedures, and interprets this Policy and Practices Statement.

1.4.1 Scope

Lleida.net may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all Credentials that have been issued or are to be issued immediately after the date of the publication of the updated version of the Policy and Practices Statement.

Notwithstanding to the provisions for changes in the Policies and Practices Statement, 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 the provisions of these Policies and Practices Statement will not affect the rest of the document in such case, said provisions will be considered not included.

1.4.2 Policy Management Authority

New versions and publicized updates of Lleida.net policies are approved by the Lleida.net Policy Management Authority. The Lleida.net Policy Management Authority in its present organizational structure comprises of members as indicated below:

Lleida.net Steering Committee of ISO 27001

Approval Committees as defined in Lleida.net ISO 27001

Only the Policy Management Authority has the ability to approve Lleida.net Policies and Practices Statement. This approval must be explicitly recorded.

1.4.3 Changes

Upon approval of a Policy update by the Lleida.net Policy Management Authority, that Policy and Practices Statement is published in the Lleida.net online Repository identified in “Document name and identification” section

The updated version is binding against all existing and future subscribers unless notice from a Subscriber is received within 30 days after publication of the updated Policy and Practices Statement. After such period the updated version of the Policy and Practices Statement is binding against all parties including the subscribers and parties relying on Advanced Electronic Signature Credentials and Registered Electronic Communication Attestation Certificates that have been issued under a previous version of the Lleida.net Policy and Practices Statement.

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

1.4.4 Version Management and Denoting Changes

Changes are denoted through new version numbers for the Policy and Practices Statement.

New versions are indicated with an integer number followed by one decimal that is zero

Minor changes are indicated through one decimal number that is larger than zero Minor changes include but are not limited to:

Minor editorial corrections

Changes to contact details

1.4.5 Publication

Lleida.net Policies and Practices Statement will be published immediately after initially approved and, as applicable, upon modification. The web address (URL) for publication is identified in "Document name and identification" section

1.4.6 Contact

Service provider	LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A.
Address	PCiTAL, Edificio H1, 2a planta B, 25003 , Lleida (SPAIN)
email	compliance@lleida.net
Phone	(+34) 973 282 300

1.5 Definitions, Acronyms and References

1.5.1 Definitions

- ‘electronic identification’ means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and

  which is used for authentication for an online service;
- ‘person identification data’ means a set of data enabling the identity of a natural or legal person, or a natural person

  representing a legal person to be established;
- ‘authentication’ means an electronic process that enables the electronic identification of a natural or legal person, or

  the origin and integrity of data in electronic form to be confirmed;
- ‘relying party’ means a natural or legal person that relies upon an electronic identification or a trust service;
- ‘public sector body’ means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
- ‘body governed by public law’ means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (1);
- ‘signatory’ means a natural person who creates an electronic signature;
- ‘electronic signature’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- ‘advanced electronic signature’ means an electronic signature which meets the requirements set out in Article 26;
- ‘qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;
- ‘electronic signature creation data’ means unique data which is used by the signatory to create an electronic signature;
- ‘certificate for electronic signature’ means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
- ‘qualified certificate for electronic signature’ means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

- ‘trust service’ means an electronic service normally provided for remuneration which consists of:
  a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
  b) the creation, verification and validation of certificates for website authentication; or
  c) the preservation of electronic signatures, seals or certificates related to those services;
- ‘qualified trust service’ means a trust service that meets the applicable requirements laid down in this Regulation;
- "electronic identification system" means a system for electronic identification whereby electronic identification means are issued to natural or legal persons or a natural person representing a legal person;
- conformity assessment body’ means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008,which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
- ‘trust service provider’ means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

- ‘qualified trust service provider’ means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;
- product’ means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
- ‘electronic signature creation device’ means configured software or hardware used to create an electronic signature;
- ‘qualified electronic signature creation device’ means an electronic signature creation device that meets the requirements laid down in Annex II
- ‘creator of a seal’ means a legal person who creates an electronic seal;
- ‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;
- ‘advanced electronic seal’ means an electronic seal, which meets the requirements set out in Article 36;
- ‘qualified electronic seal’ means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
- ‘electronic seal creation data’ means unique data, which is used by the creator of the electronic seal to create an electronic seal;
- ‘certificate for electronic seal’ means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;
- ‘qualified certificate for electronic seal’ means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III; UE 910/2014 (eIDAS);

- ‘electronic seal creation device’ means configured software or hardware used to create an electronic seal
- ‘qualified electronic seal creation device’ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;
- electronic time stamp’ means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
- ‘qualified electronic time stamp’ means an electronic time stamp which meets the requirements laid down in Article 42;
- ‘electronic document’ means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;
- electronic registered delivery service’ means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending

  and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

- qualified electronic registered delivery service’ means an electronic registered delivery service which meets the requirements laid down in Article 44;
- certificate for website authentication’ means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
- qualified certificate for website authentication’ means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;
- ‘validation data’ means data that is used to validate an electronic signature or an electronic seal;
- ‘validation’ means the process of verifying and confirming that an electronic signature or a seal is valid.

1.5.2 Acronyms

- RA: Registration Authority
- AES: Advanced Electronic Signature
- PS: Practices Statement
- IETF: Internet Engineering Task Force
- ISO International Standards organization
- ITU: International Telecommunications Union
- RFC: "Request for Comments"
- SSCD: Secure Signature Creation Device

1.5.3 Legal References

European Regulations

- • Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Regulation (EU) No 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC of 23 July 2014.
- Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015. On the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- • Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015. On the setting of minimum technical specifications and procedures for the security levels of means of electronic identification as provided for in Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

International Technical Standards

- ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ISO/IEC 29115:2013 “Information Technology - Security Techniques - Entity Authentication Guarantee Framework”. (ITU X.1254: Entity authentication assurance framework).

Spain national regulation

- Law 10/2010, of 28 April, on the prevention of money laundering and terrorist financing.
- Royal Decree 304/2014, of 5 May, approving the Regulations of Law 10/2010, of 28 April, on the prevention of money laundering and the financing of terrorism.
- Law 25/2007, of 18 October, on the conservation of data relating to electronic communications and public communications networks.
- Organic Law 3/2018, of 5 December, of protection of personal data and guarantee of digital rights.
- Law 6/2020, November 11, regulating certain aspects of electronic trusted services

South Africa national regulation

- Electronic Communications Act No. 25 of 2002
- Electronic Communications and Transactions Act No 36 of 2005
- National Credit Act No 35 of 2005
- Protection of Personal Information Act (POPI Act)

United Arab Emirates regulation

- Federal Law No. 1 of 2006 on Electronic Commerce and Transactions
- Federal Law No. 10 of 1992 the Evidence Law in Civil and Commercial Transactions (as amended by Federal Law No. 36 of 2006)

- Federal Law No. 11 of 1992 for issuing the Civil Procedures Law
- Federal Law No. (5) of 2017 On the Use of Remote Communication Technology in Criminal Proceedings
- Ministerial Resolution No. (259) of 2019 On the Procedural Manual for Regulating Litigation Using Electronic and Remote Communication Technologies in Criminal Proceedings
- Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations
- Cabinet Decision No. 10 of 2019 concerning the implementing regulation of Decree Law No 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations
- UAE Cabinet Resolution 57/2018 concerning the Executive Regulation of the Civil Procedure Law No 11 of 1992
- UAE Ministerial Resolutions No. (259) and (260) of 2019 On the Procedural Manual for Regulating Litigation Using Electronic and Remote Communication Technologies in Criminal and Civil Proceedings respectively
- The Federal Decree-Law No.45 of 2021 on Personal Data Protection ("PDPL")
- The UAE Federal Decree-Law No. 44 of 2021 establishing the UAE Data Office.

Kingdom of Saudi Arabia regulation

- Council of Ministers Decision No 80 of 7/3/1428H, approved by Royal Decree No M/18 of 8/3/1428H on Electronic Transactions

Lebanon Regulation

- Law No 81 of 2018 Relating to Electronic Transactions and Personal Data

Kingdom of Bahrain Regulation

- Legislative Decree No. 54 of 2018, Promulgating the Electronic Communications and Transactions Law.

Kuwait Regulation

- Law 20 of 2014 on Electronic Transactions

Islamic Republic of Iran regulation

- • Electronic Commerce Law by the Islamic Consultative Assembly of 1382/17/10, ratified by the Guardian Council on 1382/10/24

Sultanate of Oman regulation

- Sultani Decree 69/2008 – The Electronic Transactions Law

India regulation

- Information Technology Act,2000
- Amendments to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 to provide support for admissibility of Digital Evidence as Documentary Evidence

2 CREDENTIALS UTILIZATION

2.1 Appropriate / Allowed Uses of Electronic Signature Credentials

Electronic Signature: Main purpose of the Lleida.net Electronic Signature Credentials is to guarantee that they perform as a Signatory declared Identity factor, as well as a guarantee that these credentials can be used only under full control of the Signatory, and as an explicit will to perform the Electronic Signature by the Credentials owner.

Electronic Signature Credentials also guarantee that the generated Signature is uniquely linked to the document or contents being signed.

Authentication of Users: Lleida.net Electronic Signature Credentials can be used for specific electronic authentication transactions that support accessing web sites and other online content. The Authentication function of Lleida.net Electronic Signature Credentials can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a Lleida.net Service. Lleida.net Electronic signature Credentials are appropriate for user authentication.

2.2 Appropriate / Allowed Uses of Registered Electronic Communication Attestation Certification Service Credentials

Registered Electronic Communications dispatching: Main purpose of the Lleida.net Registered Communications Attestation Certification Service Credentials is to guarantee that they perform as a Sender Identity factor, as well as a guarantee that these credentials can be used only under full control of the Originator, and as an explicit will to perform a Registered Electronic Communication by the Credentials owner.

The most appropriate use of the Registered Electronic Communication Attestation Certification Service is the generation of a documentary proof and evidence that proves the dispatching, by Lleida.net or a third party, and the reception, by one or more recipients, of a certain electronic delivery, as well as of the moment in which both occurred, of the communication content and, where appropriate, of the access / download to / of attached documentation, with the main purpose that it can be used in legal contexts.

Authentication of Users: Lleida.net Registered Electronic Communication Attestation Service Credentials can be used for specific electronic authentication transactions that support accessing web sites and other online content. The Authentication function of Lleida.net Electronic Signature Credentials can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a Lleida.net Service, or the Identity of a Registered Electronic Communication Receiver. Lleida.net Electronic signature Credentials are appropriate for user authentication.

3 PROCEDURE CONCERNING AR VERIFICATION AUTHORITY

3.1 Who can Perform an RA Verification Procedure and Registration

Only Lleida.net as an RA Verification Authority, or those Lleida.net Business Partners appointed by a Contractual Relationship with Lleida.net as Delegated RA Verification Authorities, can perform an RA Identity Verification and Registration.

3.2 RA Identity Verification (Legal Person)

RA Verification Authority or RA Delegated Verification Authority shall identify the RA and enter a valid Contractual Relationship with the RA, what defines the role, obligations and responsibilities of the RA, prior to Registering the RA.

The Level of Assurance required for an RA Identity proofing and verification is the one defined in Article 2.1.3 of Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 as “substantial Level of Assurance”, and recommended to be as per same Article as “High Level of Assurance”,

3.3 Binding of Identity Verification between an RA (Legal Person), its Representatives (Natural Persons) and RA Credentials Issuance

A Natural Person will always be the “Representative” of the RA.

This Representative is the one who, once his/her Identity as a valid Representative for the RA has been verified, will receive RA Credentials, and will be able to delegate the exercise of the binding to other natural persons of its own RA, who will also receive their respective RA Credentials.

Binding shall be done as defined in Article 2.1.4 of Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 as “substantial Level of Assurance” and recommended to be as per same Article as “High Level of Assurance”.

4 ADVANCED SIGNATURE PROCEDURE

4.1 Signatory identification

RA shall identify the signatories prior to initiation of a signature procedure.

The minimum set of data needed in the identification is defined in Article 11 and Annexes of Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015, in accordance with Article 12(8) of Regulation (EU) No 910/2014.

RA detailed obligations on Signatories Identity Verification are set in a contractual relationship between the RA and Lleida.net (as an RA Identity Verification Authority) or between the RA and a Lleida.net Delegated RA Identity Verification Authority.

4.2 Binding of the signatory to the signed document

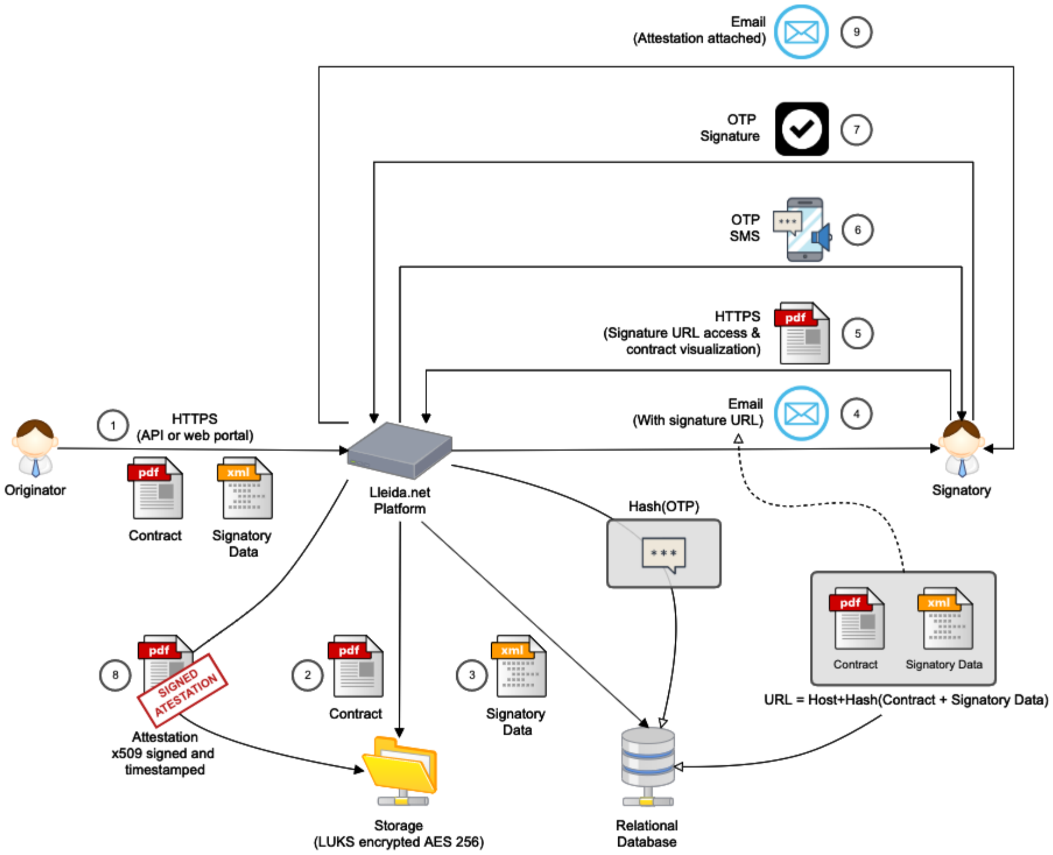
The originator makes use of electronic means to supply LLEIDA.NET with contract content and relevant electronic contact identifiers such as MSISDN (mobile phone number) and/or email address, gathered in the identification process.

A security feature separates the generation of an OTP (one-time password) signing creation data at the same time that the message containing the URL that allows to initiate the signature procedure is sent to the signatory.

OTP code is not stored in clear text at any time before the signature uses it to manifest consent introducing the code in the form presented in the signature endpoint, producing the Electronic Signature, so only the OTP is under the sole control of the Signatory. When OTP is generated by the Lleida.net system, a hash of the OTP is stored. When signatory enters the OTP, its hash is calculated and compared with the hash stored at Lleida.net system.

Once the signature has been produced, the OTP signature creation data will be stored in clear text in the Attestation as a proof for the Signatory to recognize the signature and as legal evidence for Originator and Relying Parties

The algorithm used to generate the landing page hash (unique URL identification of the endpoint of the service managing advanced signature), takes into account the hash value of the different documents to be signed as well as the identifying data of the signatory, which makes the signature data unique and guarantees the integrity of the data to be validated, and the binding of the document to the signatory.



The Lleida.net Signature Initiation procedure will validate and guarantee that all the received data have a correct format and will authorize the operation, proceeding to save the documents in encrypted storage and in a database.

During the operation of electronic document storage, their hash value will be calculated (without the metadata of the PDF Attestation Certificate, to be compatible with a hand-written biometric signature, another LLEIDA.NET service) and it will be saved in a table, together with the rest of the relevant data that uniquely identify the document

The signature service URL will contain a domain address with a prefix that will identify the Lleida.net service (for example https://sign.clickandsign.eu/h/) and a calculated part to identify the Signatory and the document to be signed, this unique part here named ”landing_hash” will be calculated from the Signatory's personal data received by the Lleida.net signature Service, and the HASH value of the document/s.

The signature service screen shown when accessing said URL displays a disclaimer message indicating that the signature will apply to all documents displayed in the signature service landing page. This screen also includes information of terms and conditions of the Advanced Signature Service itself, and of highlighted aspects of the underlying document to be signed that are relevant to consent formation.

The “landing hash” is calculated using a SHA256 algorithm with the following data:

- A document_hash that will be calculated for each document to be signed Each document _hash will be related to the unique identifier of the files in the table.
- String formed with the data set associated to the signatory in JSON string format. Usually contains telephone number, email address, first name, last name, citizen card ID, etc. among other data. These data will be provided by the Originator/Offeror at the time of initiating the signature request process, and it will be the responsibility of the Originatr/Offeror as RA to link them to the identification of the Signatory.
- contract_id: unique identifier of the Offeror that identifies the signature process.
- The date of registration of the request to start the signing process in UNIX timestamp format.
- Unique identifier of the Signatory, signatory_id.
- Unique identifier of the multi-signature, signature_id It uniquely identifies a signature process (there might be several signatories within the same signature process).

4.3 Completion of document signing

After the document has been signed, the Signatory (through an SMS or email message) and the Originator/Offeror (through the electronic means that allow communication between Requestor and LLEIDA.NET) receive the a copy of the Attestation Certificate (by email) or a URL pointing to the signature Attestation Certificate, which includes all electronic evidences and is electronically sealed and time stamped by LLEIDA.NET, including a unique Attestation Certificate ID Number.

Electronic Signature Certificate Sample

Sender and Receiver
Mobile telephone numbers, email addresses, Offeror/Source ID and destination address, as well as the corresponding IPs.

Date and time (Time Stamping)
The certificate provides the delivery and reception date and time of the different communications, as well as the actions taken.

The message Contents
The message sent by SMS or by email is also attached in the documentary evidence.

Attachments
If the message contains attachments, they will be included in the Attestation Certificate; If they are PDF's or images, they will be displayed directly on it.

Technical Annexes
The logs of the servers and communications, with all the technical information, are in the technical annex of the certificate.

Digital Signature
This document is Electronically Signed, including Time Stamping.

4.4 Operational recommendations

Lleida.net Advanced Electronic Signature Attestation Certificates are sealed, and time stamped by calculating the document hash, and encrypting it with a private key associated to an RSA X.509 version 3 certificate. LLEIDA.NET holds a legal person qualified certificate issued by an EU Qualified Electronic Signature Service Provider and could also use other valid Certification Service Providers in other countries and jurisdictions where applicable.

Any Relaying Party who trusts on LLEIDA.NET Attestation Certificates should verify that electronic seal included in it, is valid following validation rules that includes verification of Chain of Trust, Trust Service Lists and Validation Services such as OCSP or CRL.

5 REGISTERED ELECTRONIC DELIVERY ATTESTATION CERTIFICATION PROCEDURES

5.1 Addressee Identification

RA shall identify the addressee prior to initiation of a Registered Electronic Communication Attestation procedure.

The minimum set of data needed in the identification is an addressee email address or mobile phone number, that should be linked to the natural or legal person identified as the addressee by the RA.

5.2 Authorization by the RA / Originator to Lleida.net

The Originator of an Electronic Communication through Lleida.net Registered Electronic Communication Attestation service provides Lleida.net full authorization to deliver, on behalf of the Originator, the data message to the addressee designated by the Originator, and to generate and keep Registered, Electronically Signed Records and Attestation Certificates of such Electronic Communications, and to address the communication to the MSISDN (mobile phone) numbers or Email Addresses designated by the Originator, gathered in the addressee identification process

This authorization is provided by the Originator by simply using the Lleida.net Registered Electronic Communication Attestation Certification service in any of its forms (Registered Email, Registered SMS or Web-based Electronic Delivery (Openum).

5.3 Electronic Communication Dispatching and Receipt

Lleida.net considers a communication or data message has been dispatched when the message has left the last system under control of the data message Originator, or the last system under control of Lleida.net when Lleida.net performs communications and electronic records tasks on behalf of the data message Originator.

Lleida.net considers a communication of a data message has been received by the Addressee when the data message has been received at the first system under control of the Addressee (including a mobile phone terminal or the first Addressee MTA); in those cases where a Lleida.net Web system/server is used for the delivery of a web-based electronic communication, we consider the message to be received when the Addressee gains access or downloads the data message from the Lleida.net Web system/server.

5.4 Registered Electronic Communication Attestation Certification service utilization

The Originator makes use of electronic means to supply LLEIDA.NET with content and relevant electronic contact identifiers such as MSISDN (mobile phone number) or email address, gathered in the identification process

Lleida.net will make different mechanisms available to the Originator to process requests to Lleida.net to perform the Originator desired Registered Electronic Communication, attest such communication, generate the Electronic Records relevant to such communication, keep those records available for future reference, and issue relevant Registered Electronic Communication Attestation Certificates.

Registered SMS Communication: Lleida.net will make available a web interface and alternatively relevant APIs to the service, in a way that the Originator will be able to compose a message, designate an addressee as an MSISDN (mobile phone number) and request Lleida.net to initiate the dispatching of the Registered SMS message on behalf of the Originator.

Lleida.net SMSC (SMS Center), connected directly or indirectly to Telecom Operators Mobile Networks, will dispatch the message to its designated addressee, and will keep track and evidence of message contents, date and time of dispatching, and addressee.

Telecom Operator providing SMS service to the addressee (SMS Termination Services) will process the message delivery request, and will provide the Lleida.net SMSC with details on delivery to addressee terminal (mobile phone), including successful/failed delivery and date and time of delivery.

Lleida.net systems will record the addressee service provider response.

Lleida.net will Electronically Sign, using an eIDAS Qualified or other valid X.509 Certificate in other Jurisdictions, a “Registered SMS Attestation Certificate”, identifying:

- - Unique Registered Communication Transaction Identifier
- - Originator of the SMS message as per RA Identity Verification records
- - Date and Time of dispatching the SMS message
- - Addressee MSISDN (phone number)
- - Date and Time of message reception at addressee terminal (mobile phone)
- - Content of the transmitted SMS message

This Registered SMS Attestation Certificate will be stored encrypted in an encrypted storage, and made available for future reference.

Registered Email Communication: Lleida.net will enable the Originator Email Address, as per the RA Identity Verification records, to send Email messages to the Lleida.net Registered Email service system.

Using any email or SMTP capable application, the Originator will provide Lleida.net with:

- - Email message content and attachments to be delivered to the Addressee
- - Addressee Email address

These details will be provided in either of three ways:

- - By sending the message to the Addressee and sending Lleida.net Registered Email System a copy of the message
- - By sending the message to Lleida.net and adding the Addressee Email address at the beginning of the Subject filed of the email message to be delivered
- - By using a Lleida.net Web Interface (Lleida.net Mailer system or Lleida.net Openum system) to compose the email message and designate message addressees

When Lleida.net Registered Email service system received such a message, Lleida.net systems will process it as a Registered Email dispatching request, and will compose and deliver an Email message as follows:

- - Sender: the Unique Originator Identifier created under Lleida.net Registered Email System for the Originator in the Lleida.net Registered Email System
- - Addressee: the Email address designated by the Originator
- - Email message and Attachments: the ones defined by the Originator on his/her email request

Lleida.net will record all details of the message to be dispatched on behalf of the Originator, as well as Date and Time of dispatching.

Lleida.net MTA (Mail Transfer Agent) will dispatch the message, and will receive a response from the Addressee MTA with information on the message acceptance or rejection.

Lleida.net systems will record the addressee MTA response.

Lleida.net will Electronically Sign, using an eIDAS Qualified or other valid X.509 Certificate in other Jurisdictions, a “Registered Email Attestation Certificate”, identifying:

- - Unique Registered Communication Transaction Identifier
- - Originator of the Email message as per RA Identity Verification records
- - Date and Time of dispatching the Email message
- - Addressee Email address
- - Date and Time of message reception at addressee MTA (mailbox)
- - Content of the transmitted Email message, including message and all its attachments

This Registered Email Attestation Certificate will be stored encrypted in an encrypted storage, and made available for future reference

Registered Web-based Communication (Openum): Registered Communication Originator will use his/her Originator credentials to access the Lleida.net Registered Web-based Communication (Openum) service.

From this web interface, Originator will provide Lleida.net service with the following details:

- - Mechanism to notify the Addressee of the new Web-based communication available to the Addressee (Email or SMS)
- - Compose a message to the Addressee
- - Determine a Registered Communication expiration date; communication will be available to the Addressee only until this date
- - Upload any PDF documents to be transmitted to the Addressee
- - Addressee contact details in the way of an MSISDN (mobile phone number) or Email Address or both
- - An Optional shared secret or X.509 Digital Certificate to be presented by the Addressee to get access to the Registered Communication message (eg: Lleida.net Openum eIDAS)

Lleida.net service will then

- - Dispatch an Email or SMS message (as instructed by the Originator) to the Addressee, as composed by the Originator, including a link to access the PDF documents uploaded by the Originator

- - Upon Addressee accessing the provided link, if an optional shared secret or X.509 Certificate was requested by the Originator, the Addressee will have to provide as requested in order to gain access to the Originator provided PDF Documents. Otherwise, Addressee will be able to access and download the PDF Documents Uploaded by the Originator.
- - Lleida.net will record and track:
    - Originator composed message, uploaded documents and designated Addressee
    - SMS and/or Email notification dispatched to the addressee
    - Date and Time of SMS and/or Email dispatching to the Addressee
    - Addressee MSISDN (mobile phone number) and/or Email Address
    - Addressee IP Address from where the PDF Documents where accessed
    - Results of shared secret or X.509 Certificate request for PDF Documents Access, if any
    - Date and time when the PDF Documents where accessed by the Addressee
    - Contents of the PDF Documents accessed by the Addressee

Lleida.net will Electronically Sign, using an eIDAS Qualified or other valid X.509 Certificate in other Jurisdictions, a “Registered Web-based Communication (Openum) Attestation Certificate”, identifying:

- - Unique Registered Communication Transaction Identifier
- Originator of the notification as per RA Identity Verification records
- Date and Time of dispatching the notification message
- - Addressee Email Address and/or MSISDN (mobile phone number)
- - Date and Time of Addressee access to the Communication contents
- - Content of the communication, including messages and PDF Documents

This Registered Email Attestation Certificate will be stored encrypted in an encrypted storage, and made available for future reference

The Web-based Communication service link URL will contain a domain address with a prefix that will identify the Lleida.net service (for example https://openum.ae/h/) and a calculated part to identify the Addressee and the documents to be accessed, this unique part here named “landing_hash” will be calculated from the Addressee contact data received by the Originator, and the HASH value of the document

5.5 Completion of Registered Electronic Communication Attestation process

After the Communication has been completed (dispatched and received) or expired (dispatched without reception by the Addressee), the Originator (through an email message) and at Originator discretion also the Addressee (through the electronic means that allow communication between Addressee and LLEIDA.NET) receive the Attestation Certificate Document corresponding to the Registered Communication, which includes all electronic evidences and is electronically sealed by LLEIDA.NET.

Registered Communications Certificate Sample

Lleida.net
Registered communication certificate
Registered SMS
Delivery details
Lleida.net

Sender and Receiver
Mobile telephone numbers, email addresses, Offeror/Source ID and destination address, as well as the corresponding IPs.

Date and time (Time Stamping)
The certificate provides the delivery and reception date and time of the different communications, as well as the actions taken.

The message Contents
The message sent by SMS or by email is also attached in the documentary evidence.

Attachments
If the message contains attachments, they will be included in the Attestation Certificate; If they are PDF's or images, they will be displayed directly on it.

Technical Annexes
The logs of the servers and communications, with all the technical information, are in the technical annex of the certificate.

Digital Signature
This document is Electronically Signed, including Time Stamping.

5.6 Operational recommendations

Lleida.net Registered Electronic Communicaiton Attestation Certificates are sealed and time stamped by calculating the document hash, and encrypting it with a private key associated to an RSA X.509 version 3 certificate. Lleida.net holds a legal person qualified certificate issued by an EU Qualified Electronic Signature Service Provider, and could also use other valid Certification Service Providers in other countries and jurisdictions where applicable

Any Relaying Party who trusts on LLEIDA.NET Attestation Certificates should verify that electronic seal included in it, is valid following validation rules that includes verification of Chain of Trust, Trust Service Lists and Validation Services such as OCSP or CRL.

6 PHYSICAL SECURITY, FACILITIES, MANAGEMENT AND OPERATIONS CONTROL

6.1 Physical security controls

Lleida.net has implemented a Certified Information Security Management System (ISMS) in accordance with standard ISO/IEC 27001 which covers the trust services subject of this policy.

Therefore, Lleida.net has documented, adopted and implemented a security policy, a security organization as well as the necessary security controls following a risk analysis to mitigate potential identified risks in the following areas:

1. The adoption of a security policy What does it include the guidelines the department of Department and the set of information security policies as well as their review.

2. The implementation of organizational controls regarding the information security, with the assignment of liability for security, implementation of task segregation, information security in project management and the awareness, education and training on information security.

3. The implementation of processes for asset management, establishing an inventory thereof with an indication of acceptable use in accordance with the classification of the information processed or stored outside the company facilities and security of equipment and assets outside these facilities.

4. The implementation of physical access and software control management, network and associated services access control, management of user access, management of user registrations and deletions, management of access rights assigned to users, and management of access rights with special privileges.

5. The management of . confidential user authentication information and the and the review, withdrawal or adaptation of user access rights as well as The use of . confidential information for authentication.

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

7. The implementation of physical and environmental measures will not provide the service to such person a perimeter of physical security, physical input controls, office and resource security as well as protection against external and environmental threats.

8. Equipment security control measures, the implementation of location and protection controls for equipment, supply systems, cable security, equipment maintenance as well as procedures for taking assets from a company in the security of the to the security of equipment

9. The establishment of responsibilities operational, documentation and procedures, change management, capacity management, separation of development environments, testing and production, protection against malware.

10. Policies on backup copies, activity and supervision records, activity event recording and management.

11. Management of technical vulnerabilities and management of information security incidents and improvements, responses to security incidents of information and planning for the continuity of information security.

The aforementioned procedures are details on confidential internal documentation on Services and Security Management

6.2 Personnel Controls

The following Human Security procedures in Lleida.net have been established as per the following rules:

Prior to employment:

Verification takes into account, where permitted, the following:

- Availability of satisfactory character references;
- Verification of the applicant's curriculum vitae;
- Confirmation of claimed academic and professional qualifications;
- Independent identify verification;
- Review of criminal records.

The contractual obligations for employees or contractors reflect the organization's policies for information security in addition to clarifying and stating:

1. 1. that all employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;
2. 2. the employee's or contractor's legal responsibilities and rights;
3. 3. actions to be taken if the employee or contractor disregards the organization's security requirements defined by Lleida.net

Where an individual is hired for a specific information security role, Lleida.net makes sure the candidate:

a) has the necessary competence to perform the security role;
b) can be trusted to take on the role.

During employment:

Management requires the employees understand the information security responsibilities, as well as the understanding of the performance for the security policies.

A security awareness training program is defined. The awareness program is also updated regularly.

There is a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

1. 1. A verification that an information security breach has occurred is performed ;
2. 2. The actions are graduate taking into consideration the severity of the facts.

Security Audit Procedures

In case of termination or change of employment, information security responsibilities remain valid after termination and they are duly indicated the confidentiality period.

6.3 Security Audit Procedures

Security Audit Procedures have been established as per the following rules:

Periodical penetration tests try to identify vulnerabilities

Event logs recording of user activities are produced, kept and regularly reviewed.

Event logs should include, when relevant:

- User ID
- system activities;
- dates, times and details of key events (e.g. log-on and log-off);
- records of successful and rejected system access attempts;
- records of successful and rejected data and other resource access attempts;
- changes to system configuration;
- use of privileges;
- use of system utilities and applications;
- files accessed and the kind of access;
- activation and de-activation of protection systems.

6.4 Vulnerability analysis

Appropriate and timely action is taken in response to the identification of potential technical vulnerabilities. The following rules are followed to establish an effective management process for technical vulnerabilities:

a) The roles and responsibilities associated with the management of technical vulnerabilities, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any necessary coordination responsibilities are set out;

b) b) a time line is defined to react to notifications of potentially relevant technical vulnerabilities;

c) c) patches are tested and evaluated before they are installed If no patch is available, other controls are considered, such as:

- • turning off services or capabilities related to the vulnerability;
- • adapting or adding access controls;
- • increased monitoring to detect actual attacks;
- • raising awareness of the vulnerability;

d) d) an audit log is kept for all procedures undertaken.

6.5 6.5 Records archiving

Audit logs are used to reconstruct the significant events recorded in the LLeida.net or Registration Authority software and the user or event that gave rise to the log. The records will also be used in the framework of dispute resolution and litigation to resolve any potential conflict by checking the validity of a signature at a given time.

6.5.1 Types of archived events

LLeida.net logs and stores audit logs of all events related to the security system Advanced Electronic Signature Service. The following events will be logged:

- • Turning the system on and off.
- • Attempts to create, delete, set passwords, or change privileges
- • Login and logout attempts.
- • Attempts of unauthorized access to the system through the network.
- • Attempts at unauthorized access to the file system
- • Physical access to audit trails.
- • Changes in system configuration and maintenance.
- • Records of the applications that support the service.
- • Turning on and off the application that supports the service
- • Changes in the details of and/or your keys.
- • Records of requests for issuance and revocation of signature credentials.
- • Registrations of issuance and revocation of signature credentials
- • Service Lifecycle Related Events

Lleida.net also retains, through a non-automated or electronic procedure, the following information:

- • Physical access records.
- • System maintenance and configuration changes.
- • Reports of commitments and discrepancies.

6.5.2 Records archiving term

Lleida.net stores audit trail information for at least 10 years. Identity related documents are stored for 15 years.

Auditors have the right to access audit records.

Unauthorized deletion or modification of audit log entries is prevented by writing audit logs.

The audit procedures and evidences are kept in media that does not allow rewriting or deletion without detection This control in guaranteed with a system of chained hashes and digital signature. In the case of the logbook (on paper) periodic backups are made and techniques of that limit the possibility of manipulation or elimination of information

6.6 Recovery in case of a natural disaster or catastrophic event

6.6.1 Incidents and vulnerabilities management procedures

Management responsibilities and procedures are established to ensure a quick affective and orderly response to information security incidents. The following guidelines are considered:

1. management responsibilities are established to ensure that the following procedures are developed and communicated adequately within the organization:
    - • procedures for incident response planning and preparation;
    - • procedures for monitoring, detecting, analyzing and reporting of information security events and incidents;
    - • procedures for logging incident management activities;
    - • procedures for handling of forensic evidence;
    - • procedures for assessment of and decision on information security events and assessment of information security weaknesses;
    - • procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations;
2. The procedures established ensure that:
    - • competent personnel handle the issues related to information security incidents within the organization
    - • a point of contact for security incidents' detection and reporting is implemented;
    - • appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained

6.6.2 Business continuity after a natural disaster or catastrophic event

Lleida.net establishes, documents, implements and maintains processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation, and ensures that:

1. an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
2. documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event;

According to the information security continuity requirements, Lleida.net establishes, documents, implements and maintains:

1. 1. information security controls inside BCP and DPR;
2. 2. processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;
3. 3. compensating controls for information security controls that cannot be maintained during an adverse situation.

6.7 Service Termination

In the event that Lleida.net ceases to operate the services described in this policy, it will notify to the corresponding Supervisory Authority, the certification / assessment entity that has made its last conformity assessment, as well as all of its present clients and that they have been in the last five years, at least forty-five (45) calendar days prior to the end of the service

In the period of notice, subscribers may request access, at their own expense, to the evidence generated in their transactions with Lleida.net, who will provide them in a human-readable format. In any case, and for legal purposes, and from the expiration of the period of notice, Lleida.net proceed to file the evidence in PDF format according to the internal procedures for generation and preservation of evidence in force.

Given the nature of the own generated evidence and the sending to customers and maintenance of the public key used for signing evidence by provider of electronic signature, service is not required to transfer the rights and obligations of the service to a third party in the event of termination of Lleida.net as a legal entity.

The actions to be carried out for the execution of the termination shall be as follows:

Notification to current subscribers and those during the last five years, at least forty-five (45) calendar days prior to the end of the service.

- Notification to service providers

Notification to the Ministry of Industry or other relevant Authorities

Deleting the private key used for the Lleida.net evidence Signature.

7

7.1 IT/Computer Security Controls

7.1.1 Specific security Technical requirements

There are a number of controls on the different components that make up the service system

Operational controls

- • All operating procedures are duly documented in the corresponding operations manuals. LLeida.net maintains a contingency plan.
- • Tools have been implemented to protect against viruses and malicious code
- • Equipment is maintained on a continuous basis to ensure availability and integrity uninterrupted.
- • There is a procedure for safely storing, deleting, and disposing of media storage, removable media and obsolete equipment

Data exchange . The following data exchanges are encrypted to ensure the confidentiality.

- • Transmission of registration data between the RA and the registration
- • Transmission of pre-registration data.
- • Communication between ARs and LLeida.net

Access control

- • Unique user identifications are used in such a way that users are
- and may be responsible for their actions
- • Rights are allocated in accordance with the rule of providing users with the least amount of information.
- • amount of system privileges they need to do their job.
- • Access rights are cancelled immediately when users change jobs or leave the organization
- • The level of access assigned to users is reviewed every three months.
- • System privileges are assigned on a case-by-case basis and end once the reason for their assignment is known assignment is no longer valid
- • LLeida.net maintains password quality guidelines.

IT security evaluation

Lleida.net performs different audits regarding the maintenance of the ISO 27001 Certification, and Qualified Trust Services Provider status in the Trusted List of European Commission.

7.2 Life-cycle security controls

7.2.1 Systems development controls

The implementation of the software for the production systems is controlled

To avoid possible problems with these systems, the following controls are applied

- • There is a formal authorization procedure for updating software libraries (including patches) in production. Authorization is granted only after ensuring that it's working properly.
- • The testing system is kept separate from the production system to ensure that works properly before it goes into production.
- A log file is kept in all library updates.
- • Previous versions of the software are preserved.
- • The purchased software is maintained at the level supported by the vendor.
- • There are procedures to include extensions on the source code.

7.2.2 Life-cycle security controls

In order to test, a large volume of data is required that is as similar as possible to the production data . LLeida.net avoids the use of production databases with personal information.

7.2.3 Network security Controls

All the security measures and controls specified for the rest of the systems apply to the network devices. The security policy for the use of networks and network services is described in the security policy of network. Users can only access the services for which they are authorized.

7.2.4 Time Sources

When some information on time is included, the official time provided by the ROA (Real Observatorio de la Armada – Royal Army Observatory) will be used as a reference . The systems of LLeida.net will be synchronized through NTP with the ROA servers or alternatively they will be able to obtain the UTC information from the GPS satellite system which has a precission better than 100 nanoseconds with respect to all the national metrology laboratories, including the ROA, and USNO (United States Naval Observatory).

8 COMPLIANCE AUDITS AND OTHER CONTROLS

LLEIDA.NET has passed different audits on its Integrated Management System in respect to several different norms. At this time, it is certified as per the following norms:

- ISO 27001
- EIDAS QERDS (Qualified Electronic Registered Delivery Service)

Lleida.net shall perform audits on the performance of its Advanced Electronic Signature Service and its Registered Electronic Communication Attestation Certification Service The audits must be condperformed by an independent auditor. Audits on all Lleida.net Trust Services shall also be performed every two (2) years, unless other provision mandates annual assessment

All audits shall verify, at least, that Lleida.net Practices are performed in compliance with this Policy and Practices Statement, with applicable mandates from any relevant Authorities and with applicable regulations, as well as the existence of a methodology to guarantee provided services quality.

9 OTHER LEGAL AND ACTIVITY MATTERS

9.1 Fees

Fees are those set out on Lleida.net's website (www.lleida.net) or in the particular agreements signed between Lleida.net and its subscribers, between Lleida.net and the appointed RAs, or between the RA appointed by Lleida.net and its subscribers, as applicable by the subscriber's contract.

Lleida.net will publish the fees applied to the provision of each one of its services on its website, what might be updated from time to time.

Lleida.net will not charge any fees for access to the information needed to verify the validity of proof issued or to these Policies and Practices Statement nor to any information which must be made public in virtue of the provisions therein.

9.2 Financial Responsibility

Lleida.net will only be liable for a breach of the obligations provided for in applicable laws and in these Policies and declaration of practices.

Lleida.net will not be liable in any way with respect to the use of proof issued for any use not authorized by these Policies and declaration of practices.

Lleida.net is not liable for the content of the documents and data its services are used for, and will not be responsible for any damages caused in transactions when they are used.

Lleida.net in no way represents the Signatories, document generators, Relying Parties or users of the Services or issued proof or evidence.

Lleida.net does not provide any guarantee or assume any liability whatsoever towards holders of certificates or any other proof issued or towards users thereof except as established in these Policies and Practices Statement.

Lleida.net and its subsidiaries are insured under the Professional Indemnity Policy for seven million euros (€7,000,000.00).

9.3 Confidentiality of information

Confidential information shall be deemed to be any information that can be disclosed orally, in writing or by any other means or medium, tangible or intangible, currently known or that makes possible the state of the art in the future, exchanged as a consequence of the performance of the service, in which one party indicates or designates the other as confidential The parties undertake to adopt the appropriate measures to ensure the confidential treatment of such information, measures that shall not be less than those applied by them to their own confidential information, assuming the following obligations:

1.To use the confidential information only for the use which is intended.

2.To allow the access to confidential information only to those individuals or legal entities that in the provision of their services need the information for the development of tasks in which the use of this information is strictly necessary.

In this regard, the party receiving the information will warn those natural or legal persons of their obligations regarding confidentiality, ensuring compliance with them.

Communicate to the other party any breach of information of which they have or come to have knowledge, produced by the violation of this stipulation or infidelity of the persons who have accessed the confidential information, on the understanding that such communication does not exempt the party who has breached this commitment of confidentiality, from liability, but if the breach will give rise to any responsibilities arising from such omission in particular.

To limit the use of the confidential information exchanged for the parties to that which is strictly necessary in order to fulfil the object of this agreement with each party receiving confidential information assuming responsibility for any object by them or the individuals or legal entities which they allow access to the confidential information.

Not to reveal, the information of the other part to third persons except previous and written authorization of this other part.

Without prejudice to any obligations imposed by national laws and/or assumed by the party receiving the confidential information, the confidentiality obligations outlined in this clause shall not be applicable to any information in relation to which the receiving party may prove:

- That was in the public domain at the time it was disclosed.
- That after having been disclosed, was published or otherwise became public domain, without breach of the obligation of confidentiality by the party receiving such information.
- That, at the time it was disclosed, the party who received it was already in possession of it by lawful means or had the legal right to access it.
- That it had prior written consent from the other party to disclose the information.
- That it has been requested by the competent Administrative or Judicial Authorities that must pronounce on total or partial aspects of the same, in which case, the party that has to make the presentation must communicate it to the other party prior to said presentation taking place.

9.4 Personal Data Protection

As a consequence of the provision of Services, it is possible that LLEIDA.NET has access to personal data for which the Originator is responsible.

LLEIDA.NET informs the Signatory and the Originator of the processing of personal data collected in every contract and those that may be obtained during its validity in order to provide the service requested and billing for it. The legal basis for data processing is the contract between Originator and LLEIDA.NET. The data provided will be saved throughout the commercial relationship or for the necessary years to comply with all legal obligations. The data will not be transferred to third parties except in cases where there is a legal obligation. The Signatory has the right to obtain confirmation as to whether LLEIDA.NET is processing their personal data, and therefore has the right to access their personal data, rectify inaccurate data or request its deletion when the data are no longer necessary, proving their identity and interest in those actions. Personal data will not be transferred to a third country The Signatory has the right to file a complaint with the Privacy Authority (in Spain AEPD) or other applicable competent authorities in other Jurisdictions, in the event that he or she considers that his or her data protection rights are being infringed (EU Regulation 2016/679, of 27 April 2016).

9.5 Intellectual Property Rights

The entirety of the applications or computer programs that make possible the provision of the Services, including the design of the platform, its databases, navigation structure, texts, images, animations, logos or names, are the property of LLEIDA.NET or, when indicated, correspond to third parties that authorize their use and integration into the platform, and are protected by laws and treaties on intellectual and industrial property.

Any reproduction, transformation, distribution of said contents, as well as any act of decompilation or reverse engineering, outside the visualization, reproduction or edition of documents, within the LLEIDA.NET platform is prohibited. Under no circumstances will any extraction, reuse and/or exploitation of said contents be permitted which imply acts contrary to normal exploitation of the same, especially their use for commercial or promotional purposes, outside the Service or which prejudice the moral or exploitation rights of the clients of LLEIDA.NET. The Originator, as a LLEIDA.NET client shall not carry out or allow to be carried out any act that may in any way undermine or depreciate the value or validity of the intellectual and industrial property rights of LLEIDA.NET.

9.6 Obligations

Originator will have the right to use the strictly contracted Services, taking responsibility for the content of the information that is transferred through it.

Terms of the license for the program Tools (www.tools.LLEIDA.NET) and other tools provided by LLEIDA.NET to Originators LLEIDA.NET grants Originators a non-exclusive license to use these applications for the CLIENT's own purposes and for the entire duration of the Contract. The Originators may not distribute commercially, sub license, resell or transfer in any case without the prior written consent of LLEIDA.NET, nor reproduce for these purposes the programs or any modification or derivation thereof, either isolated or in conjunction with any other product or program. In addition, the Originators may not modify the programs except for personal and personal use AND for internal commercial purposes

Law of electronic commerce Originators accepts, in accordance with the provisions of Articles 21 and 22 of the LAW OF SERVICES OF THE COMPANY OF INFORMATION AND ELECTRONIC COMMERCE, LSSICE (Law 34/2002 of 11 July - B.O.E. 12 July 2.002) that they may not use the Services to send mass messages (SPAM, advertising, promotional or commercial messages) without the express consent or authorization of each of the addressees, unless there are legally stipulated exceptions, as well as the sending of messages whose purpose or content may be considered contrary to the law, morality, good customs or those constituting a crime or misdemeanour and those that may damage the rights or image of LLEIDA.NET or third parties.

Originators must keep secret the access codes to the Services and change them if he suspects that third parties have known or unduly know them.

If Originator does not comply with any of its legal and/or contractual obligations, LLEIDA.NET reserves the right to interrupt the Services immediately, informing its CLIENT that the non-compliance must be corrected so that the Services can be restored. If Originators do not correct the breach within five (5) days from the date of its communication by LLEIDA.NET, this may terminate the Contract, with the obligation for Originators to compensate for damages caused as a result of such breach.

The re-distribution of services to third without the express consent of LLEDIA.NET, in writing, is strictly prohibited.

9.7 Responsibility Waivers

LLEIDA.NET is not responsible for violations of existing legislation that may commit Originators as a result of improper use of the Services If LLEIDA.NET detects the existence of any irregularity in the use of the Services, it may terminate the contract without prior notice to the CUSTOMER.

The liability of LLEIDA.NET in any of the cases of non-compliance attributable to it will be limited to the amount of services provided object of claim.

Given that LLEIDA.NET depends on the services of third parties for the adequate provision of its own services, LLEIDA.NET declines all liability for damages caused by the fault of those, accepting only those caused by an inadequacy of the telematic means of support or the negligent action of LLEIDA.NET and its employees, duly accredited.

Given that the greater of the facilities necessary for the correct functioning of the network depend on About us THIRD companies, LLEIDA.NET is not responsible for the results of the service. This includes routing errors, loss of information or data, delays in delivery or unplanned interruptions of the Services.

LLEIDA.NET declines all responsibility related to the quality, accuracy, reliability, correctness of data, programs and information of any kind circulating on their networks. The content of such information is the sole responsibility of the parties exchanging it (sender and recipients).

LLEIDA.NET shall not be liable in the event of unauthorized use of the Services by third parties.

9.8 Liabilities

Lleida.net will be liable for damages caused to the signatory or third parties in good faith when fails to comply with the obligations imposed by Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and the national legislation of the relevant markets applicable to this service.

The liability of the trusted service provider regulated by law shall be enforceable in accordance with the general rules on contractual or non-contractual fault, as the case may be, but it shall be for the trusted service provider to prove that he acted with the professional diligence required of him by being liable for damage caused intentionally or negligently to any natural or legal person to whom he has delegated this service.

When LLeida.net as a trusted service provider, duly and in advance report to the applicants, signatories and other subscribers to the service on the limitations on the use of the services it provides and these limitations. Limitations are recognizable to a third party; the trusted service provider shall not be liable to damage caused by a use of the services which goes beyond the limitations indicated.

LLeida.net as a provider of advanced electronic signature services will assume responsibility to third parties for the actions of people who delegate the execution of any or some of the functions necessary for the provision of reliable services.

Registration Authority

The Registration Authority shall assume full responsibility for the correct identification of the data applicants and signatories and verification of their data, with the same limitations as established for LLeida.net

9.9 Loss Waivers

Lleida.net accepts no liability for damage resulting from the following circumstances:

- • In case of war, natural catastrophes or any other fortuitous event or force major: disturbances of public order, strikes in transport, cut off of electricity supply and/or telephone, computer viruses, deficiencies in telecommunications services or the use of the advanced electronic signature service commitment arising from an unpredictable technological risk.
- • Caused by the unauthorized use of the signer's signature credentials, or exceeding the limits defined in this Policy.
- • Caused by improper or fraudulent use of signature credentials issued by LLeida.net
- • LLeida.net will not be responsible for the content of electronically signed documents or any other information used in an authentication process involving an advanced electronic signature issued by LLeida.net.

9.10 Validity Period of the Policy documents

This is the current Advanced Electronic Signature and Registered Electronic Communications Attestation service Policy and Practice Statement for the advanced electronic signature and electronic communication attestation certification services offered by LLeida.net Amendments to this document will be approved by the policy approval and management body.

These modifications will be included in a document updating this Policy and Declaration of Practices, the maintenance of which is guaranteed by LLeida.net.

The updated versions of this document together with the list of modifications made can be consulted at the web address (URL) identified in “Document name and identification” section.

LLeida.net will be able to modify this document for which shall act in accordance with the following procedure:

- The amendment shall be technically, legally or commercially justified.
- All technical and legal implications of the new version of specifications.
- • A control of modifications shall be established to ensure that the resulting
- specifications meet the requirements that were intended to be met and that led to the change.
- • The implications that the change of specifications may have on users will be assessed
- in case they need to be informed of the change.

In the preparatory phase of audits, LLeida.net will review this document in order to ensure that it remains up to date in relation to changes that occur in the following aspects:

- Implementing legislative framework.
- Publication of standards.
- Improvements or non-conformities identified in the audits.
- Improvements made in the services or launch of new services
- Adoption of third-party products and services that integrate with those offered by LLeida.net.

LLeida.net may make changes to this document without prior notice to users, such as:

- Corrections of typographical errors in the document
- Changes in contact information.
- Changes in service specifications or conditions.

9.11 Individual notifications and communications with Lleida.net

Any notification to Lleida.net shall be mailed info@lleida.net or by ordinary mail to Lleidanetworks Serveis Telemàtics, S.A., PARC CIENTÍFIC I TECNOLÒGIC AGROALIMENTARI, ED. H1. PL 2 - 25003 LLEIDA (Spain)

Any non-registered communication will be considered to be effective from the date when Lleida.net provides a receipt acknowledgement to the sender.

9.12 Claims and jurisdiction and applicable Law

When a user wishes to file a claim with respect to Lleida.net services, this must be communicated via any of the means of contact indicated in previous section. Lleida.net will answer the claim within a maximum period of one week.

Except as per Country-specific Supplements to this Policy and Practices Statement, Originators, Signatories and Relying Parties hereby agree to be subject to the jurisdiction of the courts and tribunals of Madrid, Spain, for any dispute that may arise in relation to the provision of services by Lleida.net, expressly waiving any other jurisdiction that would otherwise correspond. If the

Signatory is a consumer, the provisions of international treaties and conventions apply. Friendly dispute resolution will always be preferred.

Except as per Country-specific Supplements to this Policy and Practices Statement, present terms and conditions shall apply and be interpreted as per Spanish Law

9.13 Miscellaneous

Advanced Electronic Signature and Registered Electronic Communication Attestation services are based in most cases in RA services managed by Originators. Nevertheless, RA services provided by LLEIDA.NET can be contracted and associated to Advanced Electronic Signature and Registered Electronic Communication Attestation services.

In the entities obliged by the AML and CTF / FATF / MENA-FATF regulations, the exercise of due diligence activities requires the obligation to carry out identification beforehand.

In other contexts of e-commerce and remote contracting, the generation of evidence allows its presentation in court but depends on the confirmation of identity in the case it would be questioned.

When attestations are used in a context that confirm the formation of a contract, the completion of an advanced electronic signature not based on a certificate or the dispatching and reception of electronic communications, all possible electronic evidence of the transaction are incorporated, such as:

- • IP from which it is accessed
- • operating system used by the user,
- • browser used by the user,
- • technical features of the communication and
- • complementary information such as mobile phone number linked to the operation when using dual factor authentication techniques.

It is important to be kept in mind that the assignment of a mobile phone number to a specific person, even on prepaid handsets, will, in most jurisdictions, require the verification of identity through mobile phone and SIM card POS.