Lleida.net Openum UAE PASS

TSP UAE_1002 Policy and Statement on Practices for the Provision of Qualified Electronic Delivery Service – Openum UAE PASS

Document Control

Description

The purpose of this document is to describe compliance with the provisions of Federal Decree-Law No. (46) of 2021 on Electronic Transactions and Trust Services and related regulations regarding the purpose and content of the services, as well as the technical aspects of the Qualified electronic delivery service provided for in the article 24 for the above mentioned law and ETSI EN 319 521.

Documentation history

Version	Date	Author	Description
1	8/05/2026	Compliance (EP)	Initial version.

Document classification and status

Document classification	Public
Status	Approved

Related documents

Description

Contents

1. Introduction

Lleida Information Technology Network Services LLC (from now on LLEIDA.NET) is a Dubai-based subsidiary of the Spanish tech company LLEIDA.NET, focused on delivering legally valid digital communication, electronic signature, and identity verification services in the UAE and the Middle East.

2. Policy and Statement of Practices for the Provision of the Qualified Electronic Delivery Service – Openum UAE PASS

This Policy governs the provision of the qualified electronic delivery service by LLEIDA.NET

2.1. Basic Statement of the Qualified Electronic Delivery Service

LLEIDA.NET Statement of the Qualified Electronic Delivery Service (OPENUM UAE PASS) sets forth the fundamental conditions and aspects of the service, which, together with other more specific conditions and aspects, are included in this document. Consequently, through this basic statement, LLEIDA.NET affirms that:

Ownership

OPENUM is a service of LLEIDA INFORMATION TECHNOLOGY NETWORK SERVICES LLC, a company whose contact details are provided in section 1.3.4 of the Trust Services Practice Statement.

Service Availability

Service availability is as described in this document.

Publication of the Policy

Users can access this policy or the version currently in effect at the URL https://www.lleida.net/en/policies

Cryptographic Mechanisms

The electronic signature for the certification of the sending and receipt of electronic mail is generated by calculating the hash using SHA256, based on X.509 version 3 certificates and RFC 3280 "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*," using qualified eIDAS certificates issued by LLEIDA.NETPKI SLU, formerly InDenova.

Validity of certifications for the transmission and receipt of electronic mail

OPENUM UAE PASS imposes no limitations on the trustworthiness of its certified electronic delivery service other than those inherent in the technologies used and the legal presumptions. LLEIDA.NET will always use the most advanced cryptographic techniques, particularly those specified in the TS 119 312 standard.

Applicability

LLEIDA.NET considers that the most appropriate use of the certified electronic delivery service is the generation of documentary evidence attesting to the sending, by a sender, and the receipt and, where applicable, the access to or download of attached content, by one or more recipients, of a specific electronic message, as well as the time at which both occurred.

Obligations

The obligations of the user parties are described in this document.

Recording of Transactions

LLEIDA.NET records its transactions and stores this information under appropriate security conditions.

Regulations

The provision of the certified electronic delivery service (OPENUM UAE PASS) by LLEIDA.NET is carried out in accordance with UAE laws, these Policies and Statement of Practices, and LLEIDA.NET internal regulations.

Liability

LLEIDA.NET liabilities and the limitations established thereon are described earlier in this document.

Complaints

All complaints from users and third parties regarding the provision of the certified electronic delivery service must be communicated to LLEIDA.NET as set forth in this document. In the event that an agreement cannot be reached between the parties, they shall submit to the courts and tribunals indicated in the "Jurisdiction" section.

Warranty and Audits

LLEIDA.NET guarantees that the provision of the Qualified electronic delivery service complies with the provisions included in these Policies and Statement of Practices. In this regard, LLEIDA.NET will conduct periodic audits of the operation of Lleida.net, in accordance with the guidelines set forth in this document.

Fees

LLEIDA.NET may charge a fee for the provision of the service, in accordance with the rates published on its website at any given time.

Partners

LLEIDA.NET may distribute the service through third parties, who must comply with the Certification Practice Statement and the service policies for the service they distribute. Their obligations and responsibilities will also be set forth in a contract.

Suppliers

LLEIDA.NET uses the services of suppliers to provide the service; specifically, these are the following:

- LLEIDA.NET PKI SLU, formerly InDenova.
- Microsoft Azure
- Digital Dubai Government Establishment

2.2. User Community

The user community for certified electronic delivery consists of the senders and recipients of electronic notifications, or third parties acting on their behalf, who demonstrate a legitimate interest. The community also includes individuals and entities that rely on the certificates issued by Lleida.net

LLEIDA.NET is responsible for the transmission or making available of the messages to recipients and for the reliable recording of their receipt, when it occurs; and, where applicable, for access to or download of attached documentation. It is also responsible for the generation and issuance of signed certificates attesting to these events and the time at which they occurred.

Users are those who request a certified delivery from Lleida.net, as well as the recipients who agree to receive it. Likewise, those who rely on the issuance and receipt certifications generated by Lleida.net.

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

2.3. Uses of the service

The most appropriate use of the Qualified electronic delivery service is the generation of documentary evidence attesting to the transmission, by LLEIDA.NET or a third party, and the receipt, by one or more recipients, of a specific electronic transmission, as well as the time at which both occurred and, where applicable, access to or download of attached documentation, with the primary purpose of enabling its use in dispute resolution contexts.

2.4. Obligations

In addition to the obligations established by law and those already listed, the following specific obligations are established for the provision of the certified electronic delivery service.

Lleida.net

1. To certify the transmission of the messages or make them available to the recipient or recipients in the manner provided for in this Policy, issuing the corresponding certification.
2. Provide the appropriate means for the recipient or recipients of the shipment to securely generate the corresponding acknowledgment of receipt.
3. To validate, where applicable, the electronic signature(s) of the recipients in the manner required by the relevant Certification Policies.
4. Receive and retain delivery status certificates, using them to generate the delivery certification and making it available to the sender.
5. Use appropriate electronic signature methods and time stamps for the generation of certifications.
6. Ensure the confidentiality of transmissions by using encryption techniques where applicable.

User Parties

1. Ensure that the messages sent are based on a legal relationship with the recipients and that they are not unsolicited communications, except when the message is protected by law.
2. Provide LLEIDA.NET with reliable and up-to-date contact information for the recipients.
3. When the user is the recipient of a transmission, use appropriate electronic signature methods to generate the corresponding acknowledgment of receipt and, where applicable, to access the encrypted content.
4. Verify the validity of the electronic signatures and time stamps included in the certifications of dispatch and receipt of messages.
5. Report any anomalous event or situation related to the Qualified electronic delivery service or to the certifications issued, which could be considered a cause for the loss of their reliability.

Provider Parties

1. Ensure that the digital signature services used for the Qualified electronic delivery service are considered qualified under the TDRA Regulation.
2. Ensure that the time-stamping services used for the Qualified electronic delivery service are classified as qualified under the TDRA Regulation.
3. Provide LLEIDA.NET with the digital certificates necessary for the electronic signature and time-stamping of the documentation issued through the certified electronic delivery process.
4. Provide LLEIDA.NET with the time-stamping service for the certified electronic delivery process.
5. The aforementioned services may be provided internally by LLEIDA.NET once it expands the functionality of its trust service infrastructure.

2.5. Recording of information regarding the service

LLEIDA.NET maintains records of all relevant information regarding its operations for a period of 5 years from the end of the service provision. The records are protected to ensure their integrity and confidentiality.

The records are available to those with a legitimate interest in accessing them and to the authorities and courts that request them in accordance with the provisions of the law.

In particular, records are maintained—including the time they occurred—regarding the following events:

Requests for delivery of shipments and their outcomes;
Acknowledgments of receipt issued by recipients;
Certificates of dispatch and receipt;
Certificates of access to *online* documents.

The procedures for generating and retaining the aforementioned records are detailed in OPENUM UAE PASS internal management documentation.

2.6. Service Provision

2.6.1. Access to the service

Users may request certified electronic delivery of one or more items in the manner specified in OPENUM's internal management documentation. The service access address is https://admin.openum.ae

2.6.2. Service availability

The Qualified Electronic delivery service is available 24/7, except during scheduled maintenance, outages due to third-party services, unforeseeable events, and force majeure, in which case the interruption shall not exceed 0.5% within a monthly measurement window.

2.6.3. Service Features

The OPENUM UAE PASS Qualified Electronic delivery service will be provided in all or some of the following formats:

With notification to the recipient via email or SMS.
With authentication via UAE PASS digital certificate

In any case, the sender must provide LLEIDA.NET, under their own responsibility, with the email address and/or mobile phone number of the recipient or recipients of the delivery, as well as the attached PDF document and a brief text.

The evidence issued to the user parties will be in the following format and will contain, at a minimum, the following information:

A unique serial number;
A statement indicating the nature of the delivery status evidence and its probative value regarding receipt of the shipment and access to the document(s) sent, a summary of which is included;
The identity of the sender;
The identity of the recipient;
The date and time of the shipment and access to the document(s).

LLEIDA.NET takes the necessary technical measures to ensure that the receipts issued to users are secure and include a qualified electronic seal from and a timestamp certifying the exact date and time the receipt was generated.

2.7. Security Measures

LLEIDA.NET has implemented an information security management system certified to the ISO/IEC 27001 standard that covers the trusted services covered by this policy.

To this end, following a risk analysis, LLEIDA.NET has documented, adopted, and implemented a security policy, a security organization, and the necessary security controls to mitigate the identified risk in the following areas:

1. Adoption of a security policy, including management guidelines on information security, the set of information security policies, and their review.
2. Implementation of controls regarding organizational aspects of information security, including the assignment of security responsibilities, implementation of segregation of duties, information security in project management, and implementation of controls for mobile devices. Awareness, education, and training in information security.
3. Implementation of asset management processes, establishing an inventory of assets with an indication of acceptable use based on the classification of the information processed or stored
4. Implementation of processes for managing physical and logical access control, control of access to networks and associated services, user access management, management of user registrations and de-registrations, management of access rights assigned to users, and management of access rights with special privileges.
5. Management of confidential user authentication information, review, revocation, or modification of user access rights, as well as the use of confidential information for authentication.
6. Control of access to systems and applications, including controls restricting access to information, secure login procedures, user password management, use of system administration tools, and control of access to program source code
7. Implementation of physical and environmental security measures, establishing a physical security perimeter, physical entry controls, security of offices, workspaces, and resources, as well as protection against external and environmental threats.
8. Equipment security control measures, implementation of equipment location controls and protection, power supply installations, cabling security, equipment maintenance, as well as procedures for removing assets from company premises and for securing equipment and assets outside the facilities.
9. Establishment of responsibilities, documentation, and operating procedures; change management; capacity management; separation of development, testing, and production environments; protection against malicious code
10. Backup policies, activity logging and monitoring, and logging and management of activity events.

11. Management of technical vulnerabilities and information security incident management and improvements, response to security incidents, and information security continuity planning.

The aforementioned procedures are detailed in OPENUM UAE PASS confidential internal management documentation.

2.8. Notification of Changes

LLEIDA.NET will notify its user community of any changes that may affect service acceptance as follows:

- An email explaining the change must be sent to the users concerned.
- Only in certain cases, depending on the magnitude of the modification, will a prominent notice be posted on the website for as long as deemed reasonable.

3. Termination

In the event that LLEIDA.NET ceases to operate the services described in this policy, it will notify the relevant Supervisory Authority, the certification body that conducted its most recent conformity assessment, as well as all current customers and those who have been customers in the past five years, with at least forty-five (45) calendar days' notice prior to the termination of the service.

During the notice period, customers may request access, at their own expense, to the evidence generated from their transactions with Lleida.net, which will provide it in a human-readable format. In any case, and for all applicable legal purposes, upon the expiration of the notice period, LLEIDA.NET will archive the evidence in PDF format in accordance with the current internal procedures for the generation and preservation of evidence.

Given the nature of the evidence generated, the fact that it is sent to customers, and the maintenance of the public key used for signing evidence by the digital signature provider, it is not necessary to transfer the rights and obligations of the service to a third party in the event of the dissolution of LLEIDA.NET as a legal entity.

The actions to be taken to effect the termination shall be as follows:

- Notification to current service customers and those who have been customers in the last five years, at least forty-five (45) calendar days prior to the termination of the service.
- Notification to service providers.

- Notification to the Ministry of Industry.
- Deletion of the private key used for signing evidence.