LLEIDA.NET Click&Sign OTP

TSP UAE 1003 Policy and Statement of Practices for the Provision of Electronic Signature Services Using OTP – Click&Sign

This document contains confidential information and material owned by LLEIDA INFORMATION TECHNOLOGY NETWORK SERVICES LLC

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 (article 19) and related regulations regarding the purpose and content of the services, as well as the technical aspects of the Advanced Electronic Signature service provided for in the ETSI EN 319 401.

Documentation history

Version	Date	Author	Description
1	8/5/2026	Eva Pané	Initial version.

Document classification and status

Document classification	Public
Status	Approved

Related documents

Description

©LLEIDA.NET. All rights reserved. In particular, reproduction, communication, or access by unauthorized third parties is prohibited.

Lleida.net

Contents

1. Introduction 1

2. Policy and Statement of Practices for the Provision of the Electronic Signature Service via OTP – Click&Sign 2

2.1. Basic Service Statement for Electronic Signatures 2

2.2. User Community 4

2.3. Uses of the service 4

2.4. Obligations 5

2.5. Recording of information regarding the service 6

2.6. Service Provision 6

2.6.1. Access to the service 6

2.6.2. Service Availability 7

2.6.3. Service Features 7

2.7. Security Measures 9

2.8. Notification of Changes 10

3. Termination 10

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 Electronic Signature Service via OTP – Click&Sign

This Policy governs the provision of the electronic signature service via OTP by LLEIDA.NET through the Click&Sign service.

2.1. Basic Service Statement for Electronic Signatures

The Basic Declaration of the Electronic Signature Service via OTP (CLICK&SIGN OTP) by LLEIDA.NET sets forth the fundamental terms and conditions of the service, which, together with other more specific terms and conditions, are included in this document. Consequently, through this basic declaration, LLEIDA.NET affirms that:

Ownership

CLICK&SIGN is a service of LLEIDA INFORMATION TECHNOLOGY NETWORK SERVICES LLC, a company whose contact details are provided in section 1.3.4 of the Certification Practice Statement.

Service Availability

Service availability is as described in this document.

Publication of the Policy

Users will have access to this policy or the version applicable at any given time at the URL https://www.lleida.net/en/policies

Cryptographic mechanisms

The electronic signature of the evidence of transmission and receipt of electronic messages 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 EIDAS qualified certificates issued by LLEIDA.NET PKI SLU, formerly InDenova.

Validity of electronic signature evidence

CLICK&SIGN OTP imposes no limitations on the trustworthiness of its certified electronic signature service other than those inherent in the technologies used and 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 electronic signature service is the generation of documentary evidence attesting to the transmission by a sender, the receipt, and, where applicable, the signature by one or more signatories of a specific document in PDF format, 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 electronic signature service (CLICK&SIGN OTP) by LLEIDA.NET is carried out in accordance the UAE laws, these Policies and Statement of Practices, and LLEIDA.NET's internal regulations.

Liability

LLEIDA.NET's 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 certified 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 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 Policy 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:

- LLEIDANET PKI SLU, formerly InDenova.
- Microsoft Azure

2.2. User Community

The user community for electronic signatures consists of the document senders and signers, or third parties acting on their behalf, who can demonstrate a legitimate interest. The community also includes individuals and entities that rely on the evidence issued by LLEIDA.NET

LLEIDA.NET is responsible for sending or making documents available to signers and for the reliable recording of their signatures when they are made. It is also responsible for generating and issuing signed evidence attesting to these facts and the time at which they occurred.

User parties are those who request that LLEIDA.NET perform an electronic signature, as well as the signers who agree to receive it. Likewise, those individuals who rely on the electronic signature evidence 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 advanced electronic signature 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 signatories, 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 signatory or signatories in the manner provided for in this Policy, issuing the corresponding certification.
2. Provide the appropriate means for the sender or senders of the shipment to securely generate the corresponding acknowledgment of receipt.
3. To validate, where applicable, the electronic signature(s) of the signers 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, using encryption techniques where applicable.

User Parties

1. Ensure that the messages sent are based on a legal relationship with the signatories 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 signatories.
3. When the user party 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 transmission and receipt of messages.
5. Report any anomalous event or situation related to the certified 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 certified electronic delivery service are considered qualified under the TDRA Regulation.
2. Ensure that the time-stamping services used for the certified 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 anyone with a legitimate interest in accessing them, as well as to authorities and courts that request them in accordance with 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 signatories;
Evidence of receipt, forwarding, and delivery;

The procedures for generating and retaining the aforementioned records are detailed in CLICK&SIGN's internal management documentation.

2.6. Service Provision

2.6.1. Access to the service

Users may request the certified electronic delivery of one or more documents in the manner provided for in CLICK&SIGN OTP internal management documentation. The service access address is https://admin.clickandsign.ae

2.6.2. Service Availability

The electronic signature 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 Click&Sign electronic signature service via OTP will be provided as follows:

The sender uses electronic means to provide LLEIDA.NET with the contract content and the relevant electronic contact identifiers, such as the mobile phone number and/or email address, collected during the identification process.

A security feature separates the generation of the data used to create an OTP (one-time password) signature from the sending of the message to the signer containing the URL that initiates the signing procedure.

The OTP code is not stored as plain text at any time before the signatory uses it to express consent by entering the code in the form presented at the final stage of the signature, thereby producing the electronic signature, so that the OTP remains under the signatory's exclusive control. When the LLEIDA.NET system generates the OTP, a hash of the OTP is saved. When the signatory enters the OTP, its hash is calculated and compared with the hash stored in the LLEIDA.NET system.

Once the signature is generated, the OTP signature creation data will be stored in plain text in the certificate, as proof for the signatory to recognize the signature and as legal evidence for the originator and the relying parties.

The algorithm used to generate the hash of the landing page (the unique URL identifier of the service endpoint managing the advanced signature) takes into account the hash values of the various documents to be signed as well as the signer's identifying data, which makes the signature data unique and guarantees the integrity of the data to be validated, as well as the link between the document and the signer.

The LLEIDA.NET signature initiation procedure will validate and ensure that all received data is in the correct format and will authorize the operation, proceeding to store the documents in encrypted storage and in a database.

During the storage of the electronic documents, their hash value will be calculated (excluding the certificate metadata in the PDF, to ensure compatibility with , a handwritten biometric signature service, another LLEIDA.NET service) and stored in a table, along with the rest of the relevant data that uniquely identifies the document.

The signature service URL will include a domain address with a prefix identifying the LLEIDA.NET service (for example, https://sign.clickandsign.ae/h/) and a calculated portion to identify the signer and the document to be signed: this unique part, referred to here as "landing_hash," will be calculated based on the signer's personal data received by the LLEIDA.NET signature service and the hash value of the document or documents.

The signature service screen that appears when the URL is accessed displays a disclaimer message indicating that the signature will apply to all documents displayed on the signature service's landing page. This screen also includes information on the terms and conditions of the advanced signature service itself and on key aspects of the underlying document to be signed that are relevant to the formalization of consent.

The "landing_hash" is calculated using an SHA256 algorithm with the following data:

- A document_hash will be calculated for each document to be signed. Each document_hash will be linked to a unique identifier for the files in the table.
- A string consisting of the set of data associated with the signer in JSON string format. It typically includes the phone number, email address, first and last name, ID number, etc., among other data. The originator/offeror is the one who provides this data when initiating the signature request process and is responsible, as an AR, for linking it to the signer's identification.
- contract_id: the offeror's unique identifier that identifies the signature process.
- The registration date of the request to initiate the signature process in UNIX timestamp format.
- Unique identifier of the signatory, signatory_id.
- Unique identifier of the multi-signature, signature_id. Uniquely identifies a signature process (there may be multiple signers in the same signature process).

In any case, the sender must provide LLEIDA.NET, under its own responsibility, with the email address of the recipient or recipients of the message,

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

- A unique serial number;
- Evidence of the status of the process and its evidentiary nature;
- The data associated with the sender;
- The data associated with the signatory;

The date and time of events throughout the entire process

LLEIDA.NET takes the necessary technical measures to ensure that the evidence issued to the receiving parties is secure and includes a qualified electronic seal and a timestamp certifying the moment it was generated, with the correct date and time.

2.7. Security Measures

LLEIDA.NET has implemented an information security management system certified to the ISO/IEC 27001 standard that covers the trust 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, access control 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 CLICK&SIGN's confidential internal management documentation.

2.8. Notification of Changes

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

- An email explaining the change must be sent to the users in question.
- 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, at least forty-five (45) calendar days 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.