Lleida.net

ECD_CO_1001.07_Signatures and Seals Validation Policy

Lleida SAS
Colombia - Bogotá

Documentation control

History of versions

Version	Date	Author	Description
1	07/3/2022	Gloria Salvador	Initial version
2	30/11/2022	Gloria Salvador	Correction to policy number
2.1	03/05/2023	Gloria Salvador	ONAC accreditation references

Distribution list

Company
Lleida SAS

Classification and status

Classification	Status
Internal Use	Approved

Documents referenced

Description

Table of contents

1. Introduction

1.1 Aim

To inform the general public of the guidelines established by Lleida SAS to provide Qualified Electronic Signature and Seal Validation Services as ECD in accordance with the provisions of Law 527 of 1999, Law 1437 of 2011 and the regulations that modify or complement them, in the territory of Colombia.

1.2 Scope

All members of Lleida SAS, Digital Certification Body, as well as all third parties identified in the scope of the Digital Certification Body Management System.

1.3 Distribution

Approved by the Management of Lleida SAS, this Policy must be accessible to all persons included in the distribution list specified in the document control, through the appropriate channels established in procedure ECD_CO-3001 - Management of the documentation repository.

1.4 Review

This Service Policy shall be reviewed and approved annually by the Lleida.net Security Committee. However, should any relevant changes take place for the Organisation, be they of an operational, legal, regulatory or contractual nature, they will be reviewed whenever deemed necessary, thus ensuring that the Policy remains adapted at all times.

2. Preliminary considerations

Qualified Services Policy for the Validation of Electronic Signatures and Seals, hereinafter referred to as the *Policy*, is a document drawn up by Lleida SAS (hereinafter referred to as Lleida.net) which, acting as a Digital Certification Entity (hereinafter referred to as ECD) contains the rules and procedures that Lleida.net applies as guidelines for providing Qualified Services for the Validation of Electronic Signatures and Seals in accordance with the provisions of Law 527 of 1999, Law 1437 of 2011 and the regulations that modify or complement them, in the territory of Colombia.

The Policy is in accordance with the following guidelines:

- Specific Accreditation Criteria for Digital Certification Bodies CEA 3.0-07 (hereinafter CEA) that must be fulfilled to obtain the accreditation as ECD, before the National Accreditation Body of Colombia (hereinafter ONAC).
- Law 527 of 1999
- Standards and protocols:

  Hypertext Transfer Protocol (HTTP)

  https://www.ietf.org/rfc/rfc2616.txt

  HTTP Over TLS (HTTPS)

  https://datatracker.ietf.org/doc/html/rfc2818

  CAdES (CMS Advanced Electronic Signatures). ETSI TS 101 733

  https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v02020p.pdf

  PAdES (PDF Advanced Electronic Signatures). ETSI TS 102 778

  https://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

  RFC 3126 Electronic Signature Formats for long term electronic signatures

  https://datatracker.ietf.org/doc/html/rfc3126

  RFC 5126 CMS Advanced Electronic Signatures (CAdES)

  https://datatracker.ietf.org/doc/html/rfc5126

  RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

  https://datatracker.ietf.org/doc/html/rfc3161

  RFC 3126 Electronic Signature Formats for long term electronic signatures

  https://datatracker.ietf.org/doc/html/rfc3126

RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

https://datatracker.ietf.org/doc/html/rfc5905

ANSI ASC X9.95 protocol ETSI TS 101 861 V1.2.1 Time stamping profile

https://www.etsi.org/deliver/etsi_ts/101800_101899/101861/01.04.01_60/ts_101861v010401p.pdf

ISO/IEC 19005-3:2012 Document Management - Electronic document file format for long term preservation - Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)

https://www.iso.org/standard/57229.html

DETAILS OF THE ENTITY PROVIDING LEGAL CERTIFICATION SERVICES

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

DETAILS OF THE REGISTERING ENTITY

The registration authority is the same digital certification service provider.

Petitions, Complaints, Claims, Applications and Appeals

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

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

- By telephone on +57 1 381 9903

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

3. Policy administration

The administration of the Service Policies is the responsibility of the Integrated Management System process.

Contact person

Name: Eva Pané Vidal
Position: ECD Supervisor
Contact telephone number: +57 1 381 9903
E-mail: compliance@lleida.net

The policies must be approved by the Security Committee, once approved it is the responsibility of the ECD Supervisor to update the latest version on the web portals.

3.1 ELECTRONIC SIGNATURE VALIDATION SERVICE POLICY

The Qualified Signature and Seal Validation Service Policy is identified by OID 1.3.6.1.4.1.1.53589.1.5.2

This document is a public document and its content is in accordance with the ETSI Technical Specification TS 119 441 (and in particular Annex A) and defines the policies and practices in the provision of qualified electronic signature/seal validation services.

4. SIGNATURE VALIDATION SERVICE COMPONENTS

4.1 ACTORS SVS

Signature Validation Client (SVC)

-Software component that provides a user interface to the application used by the signature validation service.

Application Driver (DA)

-Application providing signature validation functionality to the Signature Validation Client.

Signature validation service server (SVSServ)

-The component that implements the signature validation protocol on the SVSP side.

Signature Validation Service Protocol (SVP)

-Secure communication channel to exchange information between the DA and the SVSServ.

Signature Validation Application (SVA)

-A software component that is responsible for signature validation, which implements the validation algorithm and creates a signature validation report.

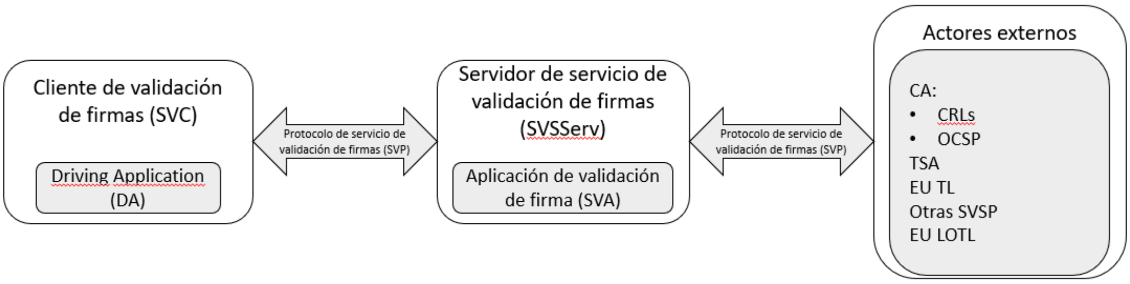
External actors

-Other sources of trust: Digital Certification Authorities, Time Stamp Authorities, List of Qualified Trusted Electronic Service Providers (TSL), the European Commission provides the list of Trusted Lists that are called upon to fulfil their purposes.

In this sense, customers who want to use the LLEIDA.NET signature validation service must implement the SVC and the DA by means of the APIS provided by LLEIDA.NET. These APIs will allow them to use the signature validation service and connect to the SVSServ in a secure way.

4.2 SERVICE ARCHITECTURE

The following diagram shows the simplified architecture of the Qualified Signature Validation Service.


Cliente de validación de firmas (SVC)
Driving Application (DA)
Protocolo de servicio de validación de firmas (SVP)
Servidor de servicio de validación de firmas (SVSServ)
Aplicación de validación de firma (SVA)
Protocolo de servicio de validación de firmas (SVP)
Actores externos
CA:
• CRLs
• OCSP
TSA
EU TL
Otras SVSP
EU LOTL

SVC:

-Executes the SVP on the user's side

-Creates the signature validation request

-Where appropriate, is concerned with the submission of the validation report.

-You can incorporate:

o A user interface to manually enter the request

oA machine interface for automated requests

o A user interface to present the report

SVSServ:

-Executes SVP and processes signature validation on the SVSP side

-Executes the VAS that:

O Implements the validation algorithm also defined in ETSI TS 119 102-1.

o It can call on external actors to fulfil its purpose.

-Creates the SVR related to the application

-Builds the signature validation response

The communication channel between the SVC and the SVSServ carries the signature validation requests response. It covers authentication of the SVSP, to avoid false reports, and supports client authentication.

5. SIGNATURE VALIDATION SERVICE DESIGN

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

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

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

Characteristics of the validation platform:

- Validation of certificates.

- Trust validation, expiry and revocation of certificates

- Validation of all certificates collected by TSL: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

- Extraction of information from certificates (identification of natural and legal persons).

    - In the case of certificates for natural persons, extraction of identification and name and surname.

    - In the case of stamp certificates, extraction of RUT and company name

    - In the case of representative certificates extraction of the above-mentioned identification data of the person and of the company

- Extraction of information on whether the certificate is qualified or not, if applicable.

- Time stamps.

- Period of validity of Time Stamps. Minimum 15 years.

- The issuance of validation evidence of electronic signature certificates shall be performed in accordance with ETSI standards.

- The issuance of validation evidence of electronic seal certificates shall be performed in accordance with ETSI standards.

- The verification of time stamps that may be received for verification, as well as the electronic certificates to be validated, shall comply with the standards in force.

- Generation and issuance of evidence.

In addition to electronic signature validation services, embedded applications are provided with the ability to extend both ASN.1 and XML and PDF electronic signatures to long-lived formats. The Service retrieves the necessary validation evidence for the extension to the desired long-lived format, and constructs the resulting signature.

In order to guarantee the reliability of an electronic signature over time, it must be complemented with information on the status of the associated certificate at the time it was produced and/or non-repudiable information incorporating a time stamp, as well as the certificates that make up the chain of trust.

This implies that, if we want to have a signature that can be validated over time, the electronic signature generated must include evidence of its validity so that it cannot be repudiated. For this type of signature, there is a service that maintains this evidence and updates the signatures before the keys and associated cryptographic material become vulnerable.

The steps performed by the service are:

1. Firstly, the produced or verified electronic signature is verified, validating the integrity of the signature, the compliance with XAdES, CAdES or PAdES standards, and the references.

2. An electronic signature completion process is carried out, consisting of the following:

a. Obtain the references to the certificates, as well as store the signatory's certificates.

b. Obtain references to and store certificate status information, such as certificate revocation lists (CRLs) or OCSP responses.

3. References to certificates and status information are stamped.

The storage of certificates and status information is done within the document resulting from the electronic signature, following the AdES -X or -A signature modalities.

For the archiving and management of electronic documents, the recommendations of international technical guidelines shall be followed.

7.1 SIGNATURE VALIDATION PROCESS REQUIREMENTS

LLEIDA S.A.S, approves the following advanced signatures/seals in CADES, XADES and PADES formats at compliance levels B, T and LT, which are recognised by the Member States.

LLEIDA S.A.S approves the conditions and policies under which the validity of an advanced electronic signature/seal is confirmed, following ETSI TS 119 101:

(1) the certificate supporting the advanced electronic signature was valid at the time of signing;

(2) the signature validation data correspond to the data provided to the relying party;

(3) the single set of data representing the user is correctly provided to the relying party;

(4) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(5) where the advanced electronic signature is created by a qualified electronic signature creation device, the use of such a device is clearly indicated to the relying party;

(6) the integrity of the signed data has not been compromised;

(7) At the time of signature, the following conditions were met:

a) be uniquely linked to the creator;

(b) allow the identification of the originator;

(c) it has been created using creation data that can be used by the creator for the creation of a signature, with a high level of confidence, under his exclusive control; and

(d) be linked to the data to which it relates in such a way that any subsequent modification of the data is detectable;

(8) the system used to validate the advanced electronic signature provides the relying party with the correct outcome of the validation process and enables the relying party to detect any relevant security issues.

7.1.1 VALIDATION MODEL

According to ETSI EN 319 102-1, the conceptual model of QES / QESeal or AdES_QC / AdESeal_QC validation is presented in Figure 1.

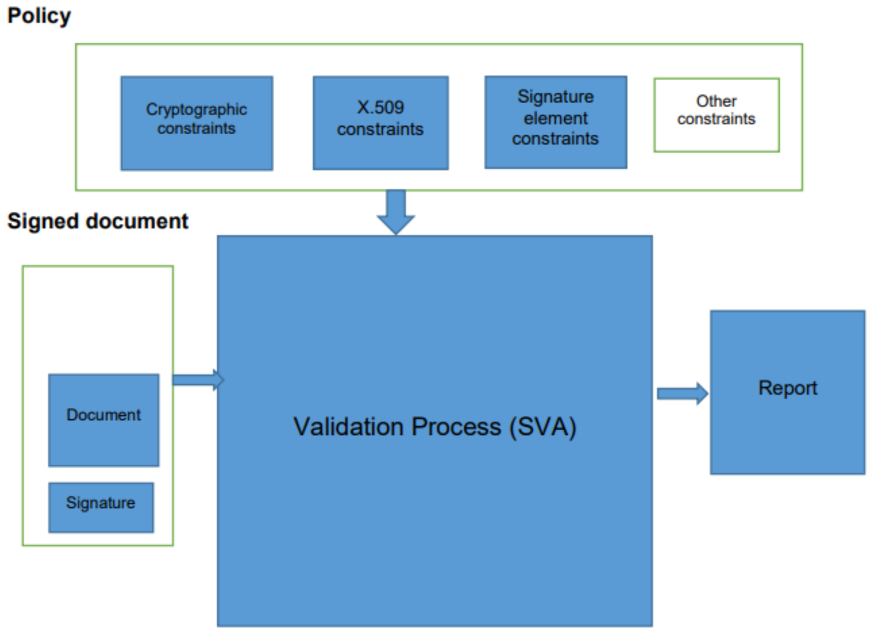


Illustration 1: Conceptual validation model

In the model, the SVA component receives the signature/stamp and, according to the Validation Policy (set of constraints), validates and generates a status indicator and a validation report which is interpreted by a user (relying party) for the applicability of the signature/stamp.

To validate the signature/stamp format, several sub-processes are executed within the SVA process (validation process for the selected format/level): format check, quality control check, cryptographic check, etc. the process is PASSED, FAILED or UNDETERMINED.

The statuses provided by the SVA process after validating the particular format/level according to the Validation Policy are:

-APPROVED : verifications of all cryptographic characteristics/parameters of the signature/seal are successful according to the Policy; it should be noted that the service indicates that the signature/seal is technically valid, but this does not mean that it is applicable for the particular business purpose;

-FAILED : the checks of all cryptographic characteristics/parameters of the signature/seal are not satisfactory, the signature/seal was created after the revocation of the QA, or the format did not match one of the specified reference formats;

-UNDETERMINED : the results of the individual checks do not allow the signature/seal to be assessed as PASSED or FAILED; acceptance of the signature/seal is the prerogative of the user/Relying Party.

For each e-signature/e-stamp level/format, the SVA performs a logical sequence of sub-processes comprising the following validation processes:

-Validation process for basic signature/stamp format - BASELINE_B. The SVA performs this process if the validation time is within the validity period of the QC and is not revoked, or the validation time is outside the validity period of the QC and the CA has provided information on its revocation/cancellation;

-Validation process for basic signature/stamp level BASELINE_T and BASELINE_LT - the SVA performs this validation process for basic signature validation of a signature/stamp with certified time (_T) and signature/stamp with certified time and status of a QC (_LT);

-Validation process for signature/stamp level BASELINE_LTA - the SVA performs this basic signature validation process of a signature/stamp with certified time (_T), of signature/stamp with certified time and status of a QC (_LT) and of a signature/stamp with archival material (LTA);

7.1.2 VALIDATION PROCESS

The process that the VAS follows is:

(1) If the signature/stamp for validation is:

-with profile BASELINE_B - the SVA shall perform (4)

-with profile BASELINE_T or BASELINE_LT - the VAS shall perform (3)

-with BASELINE_LTA profile: the VAS shall perform (2)

(2) If the VAS does not support signature/stamp validation with the BASELINE_LTA profile, the VAS shall perform (3); otherwise, the VAS shall perform a signature/stamp validation process with the BASELINE_LTA profile and go to (5);

(3) If the VAS does not support signature/stamp validation with the BASELINE_LTA, BASELINE_T and BASELINE_LT profiles, the VAS shall perform (4); otherwise, the VAS shall perform a signature/stamp validation process with the BASELINE_T and BASELINE_LT profile and proceed to (5);

(4) The SVA will perform a basic format stamp/signature validation process (BASELINE_B profile) and go to (5);

(5) When the validation status of the selected validation process is PASSED, the SVA shall return a TOTAL PASSED status indicator and a validation report in XML format as a response from the web service;

(6) When the validation status of the selected validation process is FAILED, the VAS shall return a TOTAL-FALID status indicator and a validation report in XML format as a response from the web service;

(7) Otherwise, the VAS shall return the INDETERMINATE status indicator and a validation report in XML format as a response from the web service.

Signature/stamp validation requests and responses to these requests use the secure communication channel between Client and Server. The exchange is protected by server authentication support and client authentication can be maintained. The validation protocol (requests and responses) complies with ETSI EN 119 442.

According to ETSI TS 319 172-1, the VAS performs the validation process in the following steps:

Step 1: The Customer generates and sends a validation request containing the documents (whether the signature/stamp is wrapped or unwrapped); the validation constraints are implicitly set by the SVA software and the validation process executes them according to the format of the signature/stamp delivered in the request.

Step 2: The VAS performs signature/seal validation; the implementation of this step involves the use of additional internal LLEIDA S.A.S. trust services (CRL/OCSP,) or, if necessary, other external providers.

Step 3: The VAS generates, prepares and sends an XML response as a validation report in response to a signature/stamp validation request; the detailed validation report contains the status indicator (YES/NO) of the validation of each constraint and its effects depending on the selected validation process of the VAS, complies with the technical specification ETSI TS 119 102-2.

Step 4: Based on the XML response of the validation report, the User/Trust accepts or rejects the technical validity of the signature/stamp.

The service performs the following validation processes, depending on the profile of the signature/stamp submitted:

-Signature/stamp validation process with BASELINE_B profile;

-Time stamp validation process;

-Signature/stamp validation process with BASELINE_T and BASELINE_LT profiles; this process is the same for both profiles;

-Signature/stamp validation process with BASELINE_LTA profile.

The choice of the VAS validation process follows the instructions in section 12.2 of the validation model and the selected process performs the above steps, including the basic functional procedures (sub-processes), which build the logical sequence of checks in the framework of the signature/stamp validation process.

7.1.3 RESULT OF THE VALIDATION

The signature/stamp validation process ends with:

-Validation status indicator (PASSED, FAILED, UNDETERMINED);

-Validation policy identifier (or description of limitations);

-Date and time of validation and validation data (signature / stamp certificate);

-The selected validation process (according to signature/seal profile);

-Validation report.

7.2 SIGNATURE VALIDATION PROTOCOL REQUIREMENTS

These are currently considered supported formats:

-XAdES (XML Advanced Electronic Signatures) format, according to technical specification ETSI TS 101 903, version 1.2.2, version 1.3.2. and version 1.4.1. For later versions of the standard, changes in the syntax will be analysed and the adaptation of the profile to the new version of the standard will be approved by means of an addendum to this signature policy.

-CAdES (CMS Advanced Electronic Signatures) format, according to technical specification ETSI TS 101 733, version 1.6.3, version 1.7 and version 1.8.1. For subsequent versions of the standard, changes in the syntax will be analysed and the adaptation of the profile to the new version of the standard will be approved by means of an addendum to this signature policy.

-PAdES (PDF Advanced Electronic Signatures) format, according to technical specification ETSI TS 102 778-3, version 1.2.1 (later versions will be accepted as long as they do not imply significant changes in the syntax of the tags used in this policy) and ETSI TS 102 778-4 for the case of long signatures in PADES (PAdES Long Term). Otherwise, the adaptation of the profile to the new version of the standard shall be approved by means of an addendum to this signature policy.

7.3 INTERFACES

7.3.1 COMMUNICATION CHANNEL

LLEIDA S.A.S operates and supports the SERVICE as a web service accessed through:

-API Qualified electronic signature or seal validation service: https://app.swaggerhub.com/apis/eSignaBox/circuits-api/2.0.3#/Signatures/checkSignatures

The interface uses a secure transport/communication channel that supports client authentication.

The SERVICE is authenticated through the use of tokens and Open ID Connect protocols:

API Authorisation: https://app.swaggerhub.com/apis/eSignaBox/authorization-api/2.0.1

7.3.2 SVSP - OTHER ECD

In certain cases, the SERVICE requires access to external sources of certificates related to the signature/seal validation process to a signed/sealed document. Such external (indirect) participants in the validation process are:

-Repositories of certificates held by ECD: public registers, CRL/OCSP sources; time stamping certification authorities;

-External (EU Member States) Trusted List (TL);

-List of Trusted Lists (LoTL).

The SERVICE uses standardised software interfaces to access these external sources of qualified certificates, which it verifies during the QES/QESeal and/or AdES/AdESeal_QC validation process.

The LoTL is a publication of the European Commission. This XML file contains the Member States' Trusted Lists, including the National Trusted List.

Information on who signs and publishes LoTL can be found at: http://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52015XC1224(01)&from=EN.

The signature format of the LoTL and the national TL is XAdES BASELINE_B. The SERVICE trusts LoTL by verifying the signature through the certificate published at the above address.

7.3.3 SIGNATURE VALIDATION REPORT REQUIREMENTS

The signature / seal validation process ends with:

-Validation status indicator (PASSED, FAILED, UNDETERMINED);

-Validation policy identifier (or description of limitations);

-Date and time of validation and validation data (signature / stamp certificate);

-The selected validation process (according to signature/seal profile);

-Validation report.

6. Service security policies

The service and the system that manages it address the various aspects of security:

- Insurance

The system does not allow unauthorised access to information, through the platform and direct attacks on the servers on which it runs.

- Traceable

All user actions involving a modification to a document are logged.
In some services the event audit is signed and stamped with TSA to ensure its authenticity.

- Fidedigno

The originals of the documents remain unchanged

- Integrity

The expert evidence generated remains unchanged.

- Good Information Security Practices

The certified Email Service Management System is periodically audited according to ISO 27001 standards.

- Audited

In addition, technical and Ethical Hacking reviews are carried out in accordance with OWASP.

7. Rates

Fees for services will be defined in contracts with client organisations.

8. Obligations

Obligations of the ECD Lleida.net

Lleida.net, as a certification service provider, is obliged, in accordance with the regulations in force in the Service Policies and the CPD, to:

1. Comply with the provisions of current regulations, the CPD and the Certificate Policies.
2. Publish the CPD and each of the Service Policies on the Lleida.net website.
3. Inform ONAC of modifications to the CPD and Certificate Policies.
4. Maintain the CPD and Service Policies with their latest version published on the Lleida.net website.
5. Deliver the service in accordance with the Service Policies and defined standards.

9. Map of controls

Standard	Section
CEA- 3.0-07	10.11