SPECIFIC TERMS OF USE

Universign

VERSION : **02/20**	DIFFUSION : **RESTREINT**	10/09/2020

1. Specific terms of use of electronic signature service

The purpose of these Specific Terms of Use (STU) is to define the conditions for accessing and using the Electronic Signature Service. They supplement the ToU of Universign services on which they take precedence and the Certification Policy.

Before any use of the Service, the User shall acknowledge:

- that they have read these STU;
- that they have the legal competence and authorizations to commit to the terms of these STU
- that they accept the STU without reserve.

The acceptance of the User is materialized by clicking on the check box on the Website at the time of the creation of a User account or prior to the signature.

These STU are made available by Universign on its website. They can be downloaded in PDF format.

> DEFINITIONS

- **Certification Authority (CA)**: refers to the authority in charge of the creation, the issuance, the management and the revocation of Certificates in accordance with the Certification Policy.
- **Electronic Certificate or Certificate**: designates the electronic file issued by the Certification Authority comprising the identification details of its Certificate's Holder and a cryptographic key to allow the verification of the Electronic Signature for which it is used.
- **Qualified Certificate**: means a certificate meeting the requirements of Article 28 or 38 of European Regulation No. 910/2014 of 23 July 2014
- **Certification Policy (PC)**: refers to the set of rules to which the CA conforms in order to implement the certification Service.
- **Certificate Holder**: designates the natural person or legal entity, identified in the Certificate having under their control the private key corresponding to the public key
- **Service**: refers to the set of services and software solutions that Universign undertakes to provide to the User under the terms herein.

> Article 1 – ELECTRONIC SIGNATURE SERVICE

The Electronic Signature Service allows the Signatory to have a solution for the creation of an Electronic Signature and the Client to collect it.

PROVISIONS APPLICABLE TO THE SIGNATORY

Article 1.1. – Access to the service

The Signatory can benefit from the proposed Service subject to having:

- Adapted IT equipment to access the Service;
- A valid, personal e-mail address (. of which they control access);
- A means of personal authentication accepted by Universign (ex: a personally assigned mobile phone number)

Electronic Signatures level 2 and level 3 require the issuance of a Certificate for which the Certificate's Holder is the Signatory.

Article 1.2. – Creation of a Universign account

Access to and use of the Service require the creation of a User account.

By exception, the level 1 Electronic Signature does not require the creation of User Account to the benefit of the Signatory.

Article 1.3. – Service usage

The Electronic Signature of Documents is based on the following steps:

- Step 1: Provision of the Document

  The Client, through their User Account, provides the Signatory with the Document to be signed and, if applicable adds a Document to be read.

- Step 2: Invitation to sign

  The Signatory is prompted to sign the Document through the Service.

  Where applicable, an e-mail containing a hyperlink allowing access to the Service is sent to the Signatory.

- Step 3: Access to the Document

  The Signatory is directed to an interface displaying the Document to be signed. They are prompted to read the entire Document.

- Step 4: Consent to the Document and to the STU/ToU

  The Signatory states that they have read the Document and, when the Signature is required, approves its content. The Signatory also states that they accept these STU supplemented by the ToU thus acknowledging the validity and enforceability of the Electronic Signature.

  The acceptance of the Signatory is materialized by clicking on the checkbox corresponding to these statements.

- Step 5: Signature – Authentication

  The Signatory clicks on the “sign” button to activate the Signature. To ensure the reliability of the Signature, the Signatory receives a confidential code sent on the phone number that they provided to Universign or to the Client. Upon receipt of the authentication code, the Signatory authenticates their identity by entering this code in order to create the Electronic Signature of the Document.

  The Signatory is informed and accepts that the conditions for obtaining their Electronic Signature are satisfactory to have binding legal effects and that their Electronic Signature may be legally binding on him.

Article 1.4. – Usage restriction

The Signatory undertakes to carry out first-hand and in accordance with the ToU and STU the steps that constitute the Electronic Signature. Delegating these operations, delegating the signature and the signature by order are prohibited.

PROVISIONS APPLICABLE TO THE CLIENT

Article 1.5. – Access to the Service

Access to and use of the Service by the Client require the creation of a User Account.

Article 1.6. – Service usage

The User undertakes to provide Universign with accurate information for the use of the Service.

The Electronic Signature of Documents is based on the following steps:

- Step 1: Provision of the Document

  The Client, through their User Account, provides the Signatory with the Document to be signed and, if applicable, to be read.

- Step 2: Invitation to sign

  The Client fills in the data relating to the Signatory required by the Service.

- Step 3: Access to the signed Document

  Access to the signed Document, considered as an original copy, is accessible through the Client's User Account.

Article 1.7. – Limitations of use

The Customer undertakes not to misuse the features of the Service or the means of authentication of the Signatory, in particular by filling in information relating to the Signatory that they know to be erroneous or by not allowing the Signatory to correctly view the document to be signed or by entering themselves the confidential code sent to the Signatory.
Any use of the Service not in conformity with the ToU and STU is likely to result in the unenforceability of the Electronic Signature and/or the nullity of the instrument to which it is affixed.

> Article 2 – ELECTRONIC SIGNATURE SERVICE LEVELS

The Service allows the implementation of three levels of Electronic Signatures, the legal effects of which are acknowledged by the applicable regulations in the territory of the European Union.

2.1. Electronic signature level 1

Within the framework of the implementation of the level 1 Signature, identification of the Signatory is the responsibility of the Client using the organizational processes and techniques which are their own and that they implement under their sole responsibility.

Universign authenticates the Signatory using the phone number the Signatory gave to Universign (by the Signatory themselves or by the Client), if applicable.

The Electronic Signature Level 1 does not require the creation of a Universign Account by the Signatory.

Within the framework of the use of this Signature, Universign cannot guarantee the identity of the Signatory, the only elements provided being those communicated by the Client.

The identification data which appear on the Electronic Signature are those provided to Universign by the Client.

2.2 Electronic signature level 2

Within the framework of the implementation of the level 2 Electronic Signature, verification of the Signatory's identification is carried out remotely by means of the digital copy of their identity document provided to Universign.

Universign authenticates the Signatory using the phone number of the Signatory provided to Universign (by the Signatory themselves or by the Client), if applicable.

Within the framework of the use of this Signature, Universign cannot guarantee the identity of the Signatory. Accordingly, it is the responsibility of the Client to verify by their own means and under their sole responsibility the identity of the Signatory.

Universign verifies the consistency between the identification data reported and the copy of the proof of identity which was sent to it.

The level 2 Electronic Signature is carried out by means of Certificates compliant with the standard ETSI EN 319 411-1.

2.3. Electronic signature level 3

Within the framework of the implementation of the level 3 Electronic Signature, Universign verifies the identity of the Signatory in their presence using a proof of identity.

Universign authenticates the Signatory using the phone number of the Signatory provided to Universign (by the Signatory themselves or by the Client), if applicable.

The Electronic Signature Level 3 is carried out by means of Certificates compliant with the standard ETSI EN 319 411-2.

> Article 3– STORAGE OF DOCUMENTS

Universign stores, at the request of the Client and in such a way as to preserve their integrity, the Documents signed through the Service. This storage allows the Client to consult, conserve, reproduce and/or destroy the signed Documents on line.

The purpose of the electronic preservation service is to ensure, for the duration of the storage, the integrity of the signed documents and the extension of the reliability of Electronic Signatures beyond their period of technological validity.

Universign reserves the right to store the signed Documents with a specialized commercial partner.

The Documents are stored from the date of their filing and until such time as the Client's User Account is closed.

It is up to the User to take all necessary measures to preserve the Documents which are not stored or no longer stored by the Service in a sustainable and integrated manner.

> Article 4 – OBLIGATIONS OF USERS

Article 4.1. – Obligations of the Client

The Client undertakes to:

- Ensure that the content of the Documents is lawful and does not facilitate the performance of illegal acts or acts contrary to the applicable laws and regulations;

- Ensure that the content of the Documents does not affect the privacy of the persons and/or the provisions relating to the protection of personal data and/or competition law, and/or consumer law;
- Where applicable, if the Client is a business or a professional, ensure that they comply with the obligations incumbent upon them in relation to their status, in particular in terms of legal notices and transmission of signed Documents.

The use of the Service outside of these guarantees entails the sole responsibility of the Client.

Article 4.2. – Obligations of the signatory

The Signatory undertakes to:

- Provide Universign with accurate information for the use of the Service, in particular their identification and authentication data (surname, first name, e-mail address, phone number, etc.).

Ensure the confidentiality of their Login and the confidential code(s) sent to them.

> Article 5 – LIMITATIONS OF LIABILITY

Universign does not verify the content of the Documents, and therefore cannot be held liable with regard to the value and/or the validity of the content of the Documents or the lack thereof.

Universign cannot be held liable for the consequences resulting from decisions that might be taken or actions which could be undertaken based on these Documents (regardless of whether they are signed or not).

Universign cannot be held liable for any inappropriate use of the Service in relation to regulations which may apply to the Documents.

> Article 6 – GUARANTEES AND DISCLAIMERS

Within the framework of the implementation of the level 3 Electronic Signature, Universign guarantees the use of a qualified Certificate whose issuance is subject to verification of the Signatory's identity by appropriate means and in conformity with French law.

Subject to compliance by the User with the applicable ToU and STU, Universign guarantees the enforceability, within the meaning of European regulations, of the Electronic Signatures created using the Service.

Universign in no case verifies that the Service corresponds to the laws and jurisdiction applicable to Documents. Accordingly, the provision of the Service does not exempt Users from analyzing and verifying the legal requirements and/or applicable regulatory requirements.

> Article 7 – DATA RETENTION

The log data of events relating to the Service are kept for a period of 15 years from the date of their issue. They are likely to be transmitted to administrative and judicial authorities in the event of an audit as well as to interested parties in the event of litigation relating to the validity of the Signature.

2. Specific terms of use of time-stamping service

The purpose of these Specific Terms of Use (STU) is to define the conditions for accessing and using the Time-Stamping Service. They supplement the ToU of Universign services on which they take precedence and the Time-Stamp Policy.

Before any use of the Service, the User shall acknowledge:

- that they have read these STU;
- that they have the legal competence and authorizations to commit to the terms of these STU
- that they accept the STU without reserve.

The acceptance of the User is materialized by clicking on the check box on the Website at the time of the creation of a User account.

The STU are made available to them by Universign on its website. They can be downloaded in PDF format.

> DEFINITIONS

- **Time-Stamp Authority (TSA)**: refers to the authority in charge of issuing the Time-stamp tokens under the Time-Stamp Policy.
- **Electronic Seal**: means a process which guarantees the origin and the integrity of the Document on which it is liked.
- **Time-stamp token**: means a structure that links a Document at a particular point in time, thus establishing evidence that it existed at that time.
- **Time-Stamp**: refers to a process making it possible to certify, by means of Time-stamp tokens, that a document existed at a given time.
- **Certification Policy (CP)**: refers to the set of rules to which the CA conforms in order to implement the certification service.
- **Time-Stamp Policy (STP)**: refers to the set of rules to which the STA conforms in order to implement the Time-Stamp Service.
- **Service**: refers to the set of services and software solutions that Universign undertakes to provide to the User under the terms herein.

> Article 1 – TIME-STAMP SERVICE

The Service makes it possible to time stamp Documents using Time-stamp tokens issued according to the Time-Stamp Policy which describes more precisely the implementation and organization of the Service.

Article 1.1. – Access to the Service

Access to the service requires:

- Adapted software equipment and materials to access the Service;
- A User Account.

Use of the Service through the API requires the information system of the User to be configured in accordance with the requirements of the Documentation.

Article 1.2. – Service usage

The User sends the Document to be Time-Stamped to the Service, through the API, in accordance with the Documentation.

In response to the User's query, the Service sends a Time-stamp token whose components are described in the Time-Stamp Policy.

Article 1.3. – Usage restrictions

The Service must not be used to provide evidence that an e-mail has been successfully sent to a recipient or received by him.

The Service does not constitute a service for sending electronic registered mail.

The Service must not be used for the purpose of identifying the author or the origin of the Document.

> Article 2 – GUARANTEES AND DISCLAIMERS

Subject to compliance by the User with the applicable ToU and STU, Universign guarantees the enforceability, within the meaning of European regulations, of the Time-stamp tokens created using the Service.

The Time-Stamping performed through the Service benefits from a presumption of accuracy as regards the date and the time contained in the Time-stamp token and the integrity of the Document to which this Time-stamp token relates.

The Time-Stamp Service is synchronized with coordinated universal time so that the Time-stamp tokens are accurate to within one (1) second.

The Time-stamp tokens are sealed by means of an Electronic Seal.

In the case of an event affecting the security of the Service and which could have an impact on the Time-stamp tokens, appropriate information will be made available to the Users through the publication Website.

The information needed to implement the Time-stamp tokens verification procedure described in the Time-Stamp Policy are available on the publication Website.

Universign does not guarantee that the Service is suited to the needs of the User. It is the responsibility of the User to verify this suitability, in particular by making sure that the provisions of the Time-Stamp Policy meet their own requirements.

> Article 3 – OBLIGATIONS OF THE USER

The User undertakes to verify the validity of the Time-stamp tokens upon receipt in accordance with the verification procedure described in the Time-Stamp Policy.

In addition to the cases provided for by the Time-Stamp Policy, the Time-stamp tokens can be verified for a period of five years from the date on which they were issued.

The User also undertakes to verify that the time-stamped Document is the one that is transmitted to Universign for Time-Stamping.

The Service does not keep an archive of the Time-stamp tokens issued.

> Article 4 – RESPONSABILITIES

The User undertakes to provide Universign with accurate information for the use of the Service.

Archiving the Time-stamp tokens is the sole responsibility of the User.

> Article 5 – DATA RETENTION

In accordance with the Time-Stamp Policy and the applicable regulations, Universign retains data relating to the operation of the Service for a period of six (6) years.

> Article 6 – POLICY AND STANDARDS

Universign undertakes to comply with the policies and standards listed in the following table.

1.3.6.1.4.1.15819.5.1.1	ETSI EN 319 411-1	CP of the Time-Stamp Authority
1.3.6.1.4.1.15819.5.2.2	ETSI EN 319 421	Time-Stamp Policy

These policies are published on the publication Website; they are audited according to the standard EN 319 403 by an accredited organization.

3. Specific terms of use of electronic seal service

The purpose of these Specific Terms of Use (STU) is to define the conditions for accessing and using the Electronic Seal Service. They supplement the ToU of Universign services on which they take precedence and the Certification Policy.

Before any use of the Service, the User shall acknowledge:

- that they have read these STU;
- that they have the legal competence and authorizations to commit to the terms of these STU;
- that they accept the STU without reserve.

The acceptance of the User is materialized by clicking on the check box on the Website at the time of the creation of a User account.

These STU are made available to them by Universign on its website. They can be downloaded in PDF format.

i. DEFINITIONS

- **Certification Authority (CA)**: refers to the authority in charge of the creation, the issuance, the management and the revocation of Certificates in accordance with the Certification Policy.
- **Electronic Seal**: Designates a process which guarantees the origin and the integrity of the Document on which it is liked.
- **Electronic Certificate or Certificate**: designates the electronic file issued by the Certification Authority comprising the identification details of its Certificate's Holderand a cryptographic key to allow the verification of the Electronic Seal for which it is used.
- **Qualified Certificate**: means a certificate meeting the requirements of Article 28 or 38 of European Regulation No. 910/2014 of 23 July 2014
- **Certification Policy (CP)**: refers to the set of rules to which the CA conforms in order to implement the certification service.
- **Certificate Holder**: designates the natural person or legal entity, identified in the Certificate having under their control the private key corresponding to the public key
- **Service**: refers to the set of services and software solutions that Universign undertakes to provide to the User under the terms of this instrument.

ii. Article 1 – ELECTRONIC SEAL SERVICE

The service allows the User to seal Documents in PDF format using Certificates and their associated cryptographic key.

Article 1.1. – Access to the Service

Access to the service requires:

- Adapted software equipment and materials to access the Service;
- A User Account;
- A Certificate of legal person associated with cryptographic keys in accordance with one of the Certification Policies mentioned herein.

Use of the Service through the API requires the IT system of the User to be configured in accordance with the requirements of the Documentation.

The Documentation is supplied by Universign upon request of the User after the creation of their account.

Article 1.2. – Service usage

The User sends the Document to be sealed to the Service, through the API, in accordance with the Documentation.

In response to the User's query, the Service sends the Document on which the Electronic Seal has been linked.

Article 1.3. – Usage restrictions

The Service makes it possible to create an Electronic Seal on a Document. It must not be used as proof of the consent of the Certificate's Holder of the Certificate used for the Electronic Seal. The Electronic Seal is not an electronic signature within the meaning of European regulations.

iii. Article 2 – CATEGORIES OF ELECTRONIC SEALS

The Service allows two categories of Electronic Seals, the legal effects of which are acknowledged by the applicable regulations in European Union.

2.1. Electronic seal level 1

The Electronic Seals Level 1 are created using Certificates compliant with the standard ETSI EN 319 411-1 which provides in particular for the possibility of remote verification of the Certificate Holder's identification data.

2.2 Electronic seal level 2

The Electronic Seals Level 2 category are created using Certificates compliant with the requirements of the standard ETSI EN 319 411-2.

iv. Article 3 – GUARANTEES AND DISCLAIMERS

Subject to compliance by the User with the applicable ToU and STU, Universign guarantees the enforceability, within the meaning of European regulations, of the Electronic Seals created through the Service.

Universign does not guarantee that the Service is suited to the needs of the User. It is the responsibility of the User to verify this suitability, in particular by making sure that the provisions of the Certification Policy meet their own requirements.

v. Article 4 – OBLIGATIONS OF THE USER

The User also undertakes to verify that the sealed Document is the one that was sent to Universign for the creation of an Electronic Seal.

The Service does not keep an archive of the sealed Documents.

vi. Article 5 – RESPONSABILITIES

The User undertakes to provide Universign with accurate information for the use of the Service.

Archiving the Documents is the sole responsibility of the User.

vii. Article 6 – POLICIES AND STANDARDS

Universign undertakes to comply with the policies and standards listed in the following table.

1.3.6.1.4.1.15819.5.1.3.4	ETSI EN 319 411-1	CP for the certificates of legal entities, level LCP
1.3.6.1.4.1.15819.5.1.3.5	ETSI EN 319-411-2	CP for the certificates of legal entities, level QCP-l

These policies are published on the publication Website; they are audited according to the standard EN 319 403 by an accredited organization.

4. Specific terms of use of cryptographic key management service

The purpose of these Specific Terms of Use (STU) is to define the conditions for accessing and using the Cryptographic Key Management Service. They supplement the ToU of Universign services on which they take precedence and the Certification Policy.

Before any use of the Service, the User shall acknowledge:

- that they have read these STU;
- that they consent to the STU of the Electronic Signature Service and/or to the STU of the Electronic Seal Service;
- that they have the legal competence and authorizations to commit to the terms of these STU;
- that they accept the STU without reserve.

The acceptance of the User is materialized by clicking on the check box on the Website at the time of the creation of a User account or prior to the signature.

These STU are made available by Universign on its website. They can be downloaded in PDF format.

viii. DEFINITIONS

- **Key pair**: refers to a pair of cryptographic keys consisting of a private key and a public key associated with a Certificate issued by the Certification Authority.
- **Registration File**: refers to the file based on which the request for the Certificate containing the information and supporting documents required by the CP is made.
- **Authorized Persons**: refers to persons expressly authorized by the Certificate's Holder to use the private key associated with the Electronic Seal Certificate issued in their name.
- **Certification Representative**: means the individual responsible for the life-cycle of the Electronic Seal Certificate. This is a legal representative of the Certificate's Holder or a person duly authorized to this effect by a legal representative of the Certificate Holder.
- **Certification Service**: means Universign's Certificate issuing service.

ix. Article 1 – CRYPTOGRAPHIC KEY MANAGEMENT SERVICE

The Cryptographic Key Management Service enables the Certificate's Holder to generate a Key pair associated with a Certificate and to use it remotely to sign or seal the Documents by means of an Electronic Signature or of an Electronic Seal.

Article 1.1. – Access to the service

Access to and use of the Service require:

- The creation of a User Account
- A means of personal authentication accepted by Universign (ex: a personally assigned mobile phone number)
- A subscription to the Certification Service.

The conditions for issuing, managing and revoking Certificates are laid down by the Certification Policy.

Article 1.2. – Service usage

For the creation of an Electronic Signature, the Key pair associated with the Certificate is enabled remotely after authentication of the Certificate's Holder by means of a confidential code sent to the phone number provided to Universign.

For the creation of an Electronic Seal, the Key-pair associated with the Certificate is enabled remotely after authentication of the Certificate's Holder or of an Authorized Person by means of a unique identifier.

Any use of the Key-pair by Authorized Persons is deemed to be made by the Certificate Holder.

Article 1.3. – Usage restriction

Universign does not guarantee that the Service is suited to the needs of the User. It is the responsibility of the User to verify this suitability.

x. Article 2 – OBLIGATIONS OF THE USER

The User undertakes to ensure the security of their means of authentication so as to avoid the use of the Key pair by unauthorized third parties.

They shall be particularly committed to taking the necessary measures to ensure the confidentiality of the means of activation sent by Universign and to implementing the measures to keep the Key pair under the exclusive control of the Authorized Persons.

xi. Article 3 – OBLIGATIONS OF UNIVERSIGN

Universign undertakes to generate and to enable the Certificate Holder's Key pair in a cryptographic device with algorithms which are compatible with the requirements of the CP corresponding to the Certificate.

The cryptographic key management Service allows the Certificate's Holder to keep the Key pair under their exclusive control for the creation of Electronic Signatures.

The cryptographic key management Service allows the Certificate's Holder and Authorized Persons to keep the Key pair under their exclusive control for the creation of Electronic Seals.

Universign ensures the protection of the private key of the Key pair in order to ensure its integrity and confidentiality.

Universign shall ensure by appropriate means that the Key pair can no longer be used after the Certificate has expired or been revoked.

With the exception of guarantees expressly provided for by the Agreement, Universign excludes any other express or implied guarantee including any implied guarantee of suitability for a specific use, satisfaction of requirement of the Certificate Holder.

xii. Article 4 – LIABILITY

The User shall accept sole responsibility in the case of harmful consequences caused to third parties resulting from a breach by the Certificate's Holder or by Authorized Persons under the conditions for the protection of the private key of the Key pair and/or its means of authentication.

xiii. Article 5 – INTELLECTUAL PROPERTY

A user license for the Key pair is granted to the Certificate's Holderas well as to Authorized Persons for the provision of the Electronic Signature and/or Seal Services.

xiv. Article 6 – DATA RETENTION

Universign retains the data relating to the verification of the User's identification data and the log data related to the use of Key pair are kept according to conditions consistent with the personal data protection policy available on the Publication Website.