universign

Specific Conditions of Use of the Services

These Specific Conditions of Use (hereinafter “**Specific Conditions of Use**” or “**SCU**”) are intended to define the conditions specifically applicable to the different services proposed by Cryptolog International, simplified joint-stock company (SAS) with a share capital of € 883.527 and registered office at 5–7 Rue du Faubourg Poissonnière, 75009 Paris, Paris Commercial Registry No 439 129 164 (hereinafter “**Universign**”).

DEFINITIONS

Unless otherwise provided, terms beginning with a capital letter will have the meaning attributed in this article and may be used both in the singular and in the plural, according to context.

Certification Authority (CA): refers to the authority in charge of the creation, issuance, management and revocation of Certificates under the Certification Policy.

Preservation Authority (PA): refers to the authority in charge of the conservation of Electronic Signatures, working in particular through controls carried out on these elements and methods for the extension of Signature reliability beyond their period of technological validity.

Validation Authority (VA): refers to the authority in charge of the validation of Signatures and Seals under the Validation Policy.

Bi-Key: refers to a pair of cryptographic keys composed of a private key and a public key associated with a Certificate issued by the Certification Authority.

Electronic Seal: refers to the procedure making it possible to guarantee the integrity of a sealed Document and to identify the origin of said Document through the Certificate used for its sealing.

Electronic Certificate or Certificate: refers to an Electronic Document issued by the Certification Authority including the identity of the Certificate holder and a public cryptographic key, used during Signature or Electronic Seal verification to check that the Signatory or issuer is indeed the holder of the Certificate.

Qualified Certificate: refers to a Certificate meeting the requirements of article 28 or 38 of European Regulation 910/2014 of 23 July 2014.

Client: refers to a natural or legal person (i) having subscribed to the Terms and Conditions of Sale – SaaS or (ii) having signed a separate commercial agreement with Universign.

User Account or Account: refers to the computer resources attributed to the User by Universign, allowing the former to access the Service.

Terms and Conditions of Use (TCU): refers to the terms and conditions of use applicable to all Services provided by Universign. They are available on the Website.

Specific Conditions of Use (SCU): refers to the specific conditions of use of the Service they govern. They are available on the Website.

Conservation: refers to the associated service consisting of the implementation of procedures and technologies making it possible to extend the reliability of Electronic Signatures or Electronic Seal for a fixed period.

Timestamp: refers to a structure which links a Document to a specific moment, therefore offering proof that it existed at that time.

Electronic Document or Document: refers to the set of structured data that may be electronically processed by the Service.

Documentation: refers to the functional and technical documentation provided by Universign as part of the Services’ use.

Registration File: refers to the file upon whose basis the Certificate request is made containing the information and supporting documents required by the Certification Policy.

Timestamping: refers to a process making it possible to prove that a Document existed at a given moment, through the use of Timestamps.

Authorized Persons: refers to the natural person responsible for the lifecycle of the Electronic-Seal Certificate. This is a legal representative of the Holder or a person duly mandated to this effect by a legal representative of the Holder.

Third Party: refers to any natural or legal person wishing to rely on a Certificate or Timestamp issued by a Certification Authority or to verify the validity of these Certificates or Timestamps, for their own needs.

Platform: refers to the technical infrastructure composed of all its materials, software packages, operating system, database, and environment managed by Universign or its subcontractors, on which the Software Package will be used. This allows for the provision of the Service in SaaS mode. It is remotely available directly via the internet network on the Website or through a smartphone or touchscreen tablet.

Certification Policy (CP): refers to the set of rules, identified by a number (OID), defining the requirements with which a CA complies in the implementation and provision of its services.

Preservation Policy (PP): refers to all the rules to which the PA complies for the implementation of the Conservation Service.

Validation Policy (VP): refers to all the rules to which the VA complies for the implementation of the Signature and Seal Validation Service.

Timestamping Policy (TP): refers to all the rules to which the TA complies for the implementation of the Timestamping Service.

Holder: refers to the natural or legal person identified in the Certificate, having control over the private key corresponding to the public key.

Validation Report: refers to the document issued by Universign following analysis of the Signature or Seal of a signed or sealed document.

eIDAS Regulation: refers to the Regulation 910/2014/EU on electronic identification and trust services for electronic transactions within the internal market, known as the “eIDAS” regulation.

SaaS (Software as a Service): refers to the mode of access to the Service. This access is made remotely via the internet through a connection to the shared Platform hosted on the Universign’s servers or those of its subcontractors.

Electronic Sealing or Sealing: refers to a procedure making it possible to guarantee the integrity of a sealed Document and to identify the origin of said Document through the Certificate used for its sealing.

Service(s): refers to the Electronic-Signature, Electronic-Seal or Timestamping service(s), as well as the associated services that Universign undertakes to provide to the User in SaaS mode.

Signatory: refers to the natural person hoping to conclude or having concluded a Transaction with the Client through the Service.

Electronic Signature or Signature: refers to a procedure making it possible to guarantee the integrity of the signed Document and to demonstrate the consent of the Signatory it identifies.

Website: refers to the website www.universign.com

Storage: refers to the service associated with the Universign Electronic-Signature Service consisting of the option to store Documents signed via the Service on the Platform.

Transaction: refers to the process between the Client and which may include a third party, during which an Electronic Document proposed by the Client is signed or timestamped via the Service.

User: refers to a user of the Services who may be, as applicable, a Client, its employees or subcontractors, or a third-party Signature invited to use the Services as part of their provision by a Client.

ARTICLE 1 – PURPOSE

These Specific Conditions of Use associated with the Terms and Conditions of Use define the conditions applicable to the Services.

ARTICLE 2 – CONTRACTUAL DOCUMENTS

The SCU form an indivisible whole with the TCU. They prevail in any event over any Client terms and conditions of purchase.

Universign reserves the right to modify these SCU at any time and without notice.

The applicable SCU, as well as previous versions, are permanently accessible on the Website, and in a format allowing their printing and/or download by the User.

ARTICLE 3 – TIMESTAMPING SERVICE

The Service allows for the timestamping of Documents via Timestamps issued according to the Timestamping Policy which more precisely describes the Service’s implementation and organization.

3.1. Access to the Service

The Signatory may benefit from the Service offered as long as they have:

- Suitable computer equipment to access the Service;
- A User Account.

Use of the Service through API requires the configuration of the User’s information system according to the instructions provided in the Documentation.

3.2. Use of the Service

The User delivers the Document to be timestamped to the Service, via the Universign API, in accordance with the Documentation.

In response to the User’s request, the Service delivers a Timestamp whose constituent elements are described in the Timestamping Policy.

3.3. Service description

The Service must not be used to establish proof that an email has been sent to or received by a recipient. The Service does not constitute a registered electronic-delivery service. The Service must not be used for the purpose of identifying the author or origin of the Document.

3.4. Guarantees and limitations of guarantees

Subject to the User’s respect for the applicable TCU and SCU, Universign ensures the enforceability of Timestamps created through the service, within the meaning of European regulations.

Timestamping carried out via the Service benefits from a presumption of accuracy of the date and time contained in the Timestamp and of the integrity of the Document to which said Timestamp relates.

The Timestamping Service is synchronized with universal coordinated time to ensure that Timestamps have a precision of one (1) second.

In case of any event affecting the Service's security and which may impact Timestamps, appropriate information will be provided to Users via the Website.

Universign does not guarantee the Service's suitability for the User's needs. It is the User's responsibly to verify this suitability, in particular by ensuring that the provisions of the Timestamping Policy meet its own requirements.

3.5. User's obligation

The User undertakes to verify the validity of Timestamps as of their reception according to the verification procedure described in the Timestamping Policy.

The information necessary for the performance of the Timestamp verification procedure described in the Timestamping Policy is available on the Website.

Outside of the cases provided for by the Timestamping Policy, Timestamps may be verified for five (5) years as of their issuance.

The User also undertakes to verify that the Timestamped document is indeed that transmitted to Universign for Timestamping.

The archiving of Timestamps falls under the exclusive responsibility of the User.

3.6. Data retention

In accordance with the Timestamping Policy and applicable regulations, Universign retains event logs regarding the Service's functioning for a period of six (6) years.

3.7. Policies and standards

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

1.3.6.1.4.1.15819.5.1.1	ETSI EN 319 411-1	Timestamping Authority CP
1.3.6.1.4.1.15819.5.2.2	ETSI EN 319 421	Timestamping Policy

These Policies are published on the Website. They are audited according to the EN 319 403 standard by an accredited body.

ARTICLE 4 – ELECTRONIC-SEAL SERVICE

The Service allows the implementation of two categories of Electronic Seal, whose legal effects are recognized by applicable regulations across the European Union.

4.1. – Access to the Service

Access to the Service requires:

- Suitable software and hardware equipment to access the Service;
- A User Account;
- A legal-person Certificate associated with cryptographic keys compliant with one of the Certification Policies mentioned herein.

Access to the Service through API requires the configuration of the User's information system according to the instructions provided in the Documentation.

The Documentation is provided by Universign upon the User's request, after the creation of its Account.

4.2. – Use of the Service

The User delivers the Document to be sealed to the Service, via the API, in accordance with the Documentation.

In response to the User's request, the Service delivers the Document to which an Electronic Seal has been affixed.

4.3. – Limitations of use

The Service makes it possible to attach an Electronic Seal to a Document. It must not be used to establish proof of consent from the Holder of the Certificate used for the Electronic Seal. The Electronic Seal does not constitute an electronic signature within the meaning of European regulations.

4.4. Categories of Electronic Seals

4.4.1. Level-1 Electronic Seal

Category-1 Electronic Seals are created via Certificates compliant with the requirements of the ETSI EN 319 411-1 standard, which provides in particular the possibility of remote verification of the Holder's identification data.

4.4.2 Level-2 Electronic Seal

Category-2 Electronic Seals are created via Qualified Certificates compliant with the requirements of the ETSI EN 319 411-2 standard, which provides in particular the verification of Holder supporting documents in the presence of its expressly authorized representative.

4.5. Guarantees and limitations of guarantees

Subject to the User's respect for the applicable TCU and SCU, Universign ensures the enforceability of Electronic Seals created through the service, within the meaning of European regulations.

Universign does not guarantee the Service's suitability for the User's needs. It is the User's responsibly to verify this

suitability, in particular by ensuring that the provisions of the Certification Policy meet its own requirements.
The User undertakes to provide Universign with exact information for the use of the Service.

4.6. – User's Obligations

The User also undertakes to verify that the sealed Document is indeed that transmitted to Universign for the creation of an Electronic Seal.

The archiving of sealed Documents falls under the exclusive responsibility of the User.

4.7. Data retention

Universign retains event logs regarding the Service's functioning for a period of fifteen (15) years from the sealing date.

4.8. Policies and standards

Universign undertakes to comply with the policies and standards mentioned in the following table:

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

These policies are published on the Website. They are audited according to the EN 319 403 standard by an accredited body.

ARTICLE 5 – CRYPTOGRAPHIC-KEY SERVICE

5.1. – Access to the Service

Access to the Service requires:

- The creation of a User Account;
- A means of personal authentication accepted by Universign (e.g., personally attributed cell-phone number);
- Subscription to the Certification Service.

The conditions for the issuance, management, and revocation of Certificates are provided by the Certification Policy.

5.2. – Use of the Service

For the creation of the Electronic Signature, the Bi-Key associated with the Certificate is activated remotely after authentication of the Holder via a confidential code delivered to the telephone number declared to Universign.

For the creation of the Electronic Seal, the Bi-Key associated with the Certificate is activated remotely after authentication of the Holder or of an Authorized Person via a unique username.

Uses of the Bi-Key by the Authorized Persons are deemed to be those of the Holder.

5.3. – Limitations of use

Universign does not guarantee the Service's suitability for the User's needs. It is the User's responsibility to verify this suitability.

5.4. – User's obligations

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

In particular, it undertakes to take the necessary measures to guarantee the confidentiality of the means of activation transmitted by Universign and to implement measures making it possible to retain the Bi-Key under the exclusive control of Authorized Persons.

5.5. – Universign's obligations

Universign undertakes to manage and activate the Holder's Bi-Key in a cryptographic device with algorithms compatible with the requirements of the CP corresponding to the Certificate.

The cryptographic-key management service allows the Holder to keep the Bi-Key under its exclusive control in order to create Electronic Signatures.

The cryptographic-key management service allows the Holder and Authorized Persons to keep the Bi-Key under their control in order to create Electronic Seals.

Universign ensures the protection of the Bi-Key's private key in order to guarantee its integrity and confidentiality.

Universign ensures, by appropriate means, that the Bi-Key can no longer be used after the expiry or revocation of the Certificate.

Except for the guarantees expressly provided for by the Agreement, Universign excludes any other express or implicit guarantee, including any implicit guarantee of suitability with a specific use or of satisfaction of the Holder's requirements.

5.6. – Liability

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

5.7. – Intellectual property

A Bi-Key use license is granted to the Holder, and to Authorized Persons, for the provision of Electronic-Signature and/or Seal Services.

5.8. – Data retention

Universign retains the data concerning the control of User identification data, and event logs linked to the use of the Bi-Key are retained under conditions compliant with the personal-data protection policy available on the Website.

ARTICLE 6 – ELECTRONIC-SIGNATURE SERVICE

The Electronic-Signature Service allows the Signatory to make use of an Electronic-Signature creation solution and allows the Client to collect said signature.

6.1. Provisions applicable to the Signatory

6.1.1. Access to the Service

The Signatory may benefit from the Service offered as long as they have:

- Suitable computer equipment to access the Service;
- A valid and personal email address (for which they control access);
- A means of personal authentication accepted by Universign (e.g., personally attributed cell-phone number).

Level-2 and 3 Electronic Signatures require the issuance of a Certificate for which the Holder is the Signatory.

6.1.2. Creation of a Universign account

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

By way of exception, the level-1 Electronic signature does not require the creation of a User Account for the Signatory.

6.1.3. Service description

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

Step 1: Provision of the Document

The Client, via their User Account, makes available the Document to be signed and, if applicable, attaches a Document to read, for the Signatory.

Step 2: Invitation to sign

The Signatory is invited to sign the Document via the Service If necessary, an email containing a hyperlink facilitating access to the Service is delivered to the Signatory.

Step 3: Access to the Document

The Signatory is directed to an interface displaying the Document to be signed. They are invited to read the Document in its entirety.

Step 4: Consent to the Document and the SCU/TCU

The Signatory declares having read the Document and, when the Signature is required, having approved its content. The Signatory also declares that they accept these SCU, completed by the TCU, thereby recognizing the validity and enforceability of the Electronic Signature.

The Signatory's acceptance is indicated by clicking the checkbox corresponding to these declarations.

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 delivered to the telephone number they have declared to Universign or the Client. Upon receipt of the authentication code, the Signatory authenticates themselves by entering this code in order to create the Electronic Signature of the Document.

The Signatory is informed and accepts that the conditions for the collection of their Electronic Signature are satisfactory to produce legal effects and that the Electronic Signature may be validly used against them.

6.1.4. Limitations of use

The Signatory undertakes to carry out the steps making up the Electronic Signature themselves and in accordance with the TCU and SCU. The delegation of these operations, the delegation of signature, and signature per procurationem are prohibited.

6.2. Provisions applicable to the Client

6.2.1. Access to the Service

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

6.2.2. Service description

The Client undertakes to provide Universign with exact information for the use of the Service.
The process for the Electronic-Signature of Documents is based on the following steps:
Step 1: Provision of the Document

The Client, via their User Account, makes available the Document to be signed and, if applicable, to read, for the Signatory.

Step 2: Invitation to sign

The Client fills in the data regarding the Signatory required by the Service.

Step 3: Access to the signed Document

Access to the original signed Document may be made via the Client's User Account.

6.2.3. Limitations of use

The Client undertakes not to misuse the Service's features or the Signatory authentication means, in particular by filling in information regarding the Signatory that it knows to be erroneous or by not permitting the Signatory to properly view the Document intended to be signed, or by entering the confidential code sent to the Signatory itself.

Any use of the Service not compliant with the TCU and SCU may entail the non-enforceability of the Electronic Signature and/or the nullity of the deed to which it is attached.

6.3. Levels of Electronic Signatures

The Service allows the implementation of three levels of Electronic Signature, whose legal effects are recognized by applicable regulations across the European Union.

6.3.1. Level-1 Electronic Signature

As part of the implementation of the level-1 Signature, Universign cannot guarantee the identity of the Signatory, nor their authorizations. The Client will be responsible for identifying the Signatory via its own organizational and technical processes, which it implements under its exclusive liability.

Universign authenticates the Signatory via the Signatory's telephone number as declared to Universign (by the Signatory themselves or by the Client), as applicable.

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

In the context of this Signature's use, Universign cannot guarantee the Signatory's identity – the only elements provided being those communicated by the Client.

The Identification data appearing on the Electronic Signature is that transmitted by the Client to Universign.

6.3.2. Level-2 Electronic Signature

As part of the implementation of the level-2 Electronic-Signature, the verification of Signatory Identification is carried out remotely via a digital copy of their identity document delivered to Universign.

Universign authenticates the Signatory via the Signatory's telephone number as declared to Universign (by the Signatory themselves or by the Client), as applicable.

In the context of this Signature's use, Universign cannot guarantee the Signatory's identity. As such, the Client is responsible for ensuring the Signatory's identity by its own means and under its own liability.

Universign verifies the consistency between the identification declared and the identity document for which a copy has been delivered thereto.

The level-2 Electronic Signature is made via Certificates compliant with the requirements of the ETSI EN 319 411-1 standard.

6.3.3. Level-3 Electronic Signature

As part of the implementation of the level-3 Electronic Signature, Universign verifies the identity of the Signatory in person and via an identity document.

Universign authenticates the Signatory via the Signatory's telephone number as declared to Universign (by the Signatory themselves or by the Client), as applicable.

The level-3 Electronic Signature is made via qualified Certificates compliant with the requirements of the ETSI EN 319 411-2 standard.

6.4. Guarantees and limitations of guarantees

Within the context of the implementation of the level-3 Electronic Signature, Universign guarantees the use of a qualified Certificate whose issuance is subject to the verification of the Signatory's identity via appropriate means, compliant with French law.

Subject to the Users' respect for the applicable TCU and SCU, Universign ensures the enforceability of Electronic Signatures created through the service, within the meaning of European regulations.

In no case will Universign verify that the Service corresponds to the legal regimes applicable to the Documents. Consequently, the provision of the Service does not exempt Users from the responsibility to analyze and verify applicable legal or regulatory requirements.

6.5. Document storage

Unless otherwise notified by the Client, Universign stores the Documents signed via the Service so as to preserve their integrity. Storage allows the Client to consult signed Documents online, and ensures their Conservation, return, and/or destruction.

The function of the electronic Conservation service is to guarantee, for the duration of Storage, the integrity of signed documents and the extension of the reliability of Electronic Signatures beyond their period of technological validity.

Universign reserves the right to store signed Documents with a specialist subcontractor.

If Storage is carried out by Universign and unless otherwise agreed between Universign and the Client, the Documents are stored from their filing until the occurrence of one of the following events:

- Fifteen (15) years after the date of the Document's filing;
- The closure of the User Account;
- Two (2) months after the end of a Contract, unless it is extended by a period of reversibility.

It is the User's responsibility to take any provisions so as to conserve Documents no longer stored by the Service in a way that is durable and ensures their integrity.

6.6 Users' obligations

6.6.1. Client's obligations

The Client undertakes to ensure:

- That the content of the Documents is legal and will not allow the performance of illegal acts or those contrary to applicable laws and regulations;
- That the content of the Documents does not infringe on the privacy of persons and/or the provisions relating to the protection of personal data and/or competition law, and/or consumer law;
- If applicable, if the Client acts as a trader or professional, that it respects the obligations imposed thereupon with regard to its status, particularly in terms of compulsory mentions and the transmission of signed Documents.

The use of the Service outside of these guarantees engages the Client's exclusive liability.

6.6.2. – Signatory's obligations

The Signatory undertakes to:

- To provide Universign with exact information for the use of the Service, in particular its identification and authentication data (full name, email address, telephone number, etc.);
- To ensure the confidentiality of its username or confidential code(s) delivered thereto.

6.7. Limitation of liability

Universign does not control the content of Documents and as such its liability may not be engaged with regard to the value and/or validity of the content of Documents, or lack thereof.

Universign's liability may not be engaged for consequences of decisions that may have been taken or actions that may be undertaken based on these Documents (whether signed or not).
Universign cannot be held liable for inappropriate use of the Service with regard to the regulations applicable to Documents.

6.8. Policies and standards

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

1.3.6.1.4.1.15819.5.1.3.3	ETSI EN 319 411-1	CP for natural-person certificates, LCP level
1.3.6.1.4.1.15819.5.1.3.1	ETSI EN 319-411-2	CP for natural-person certificates, QCP-l level

These policies are published on the publication Site. They are audited according to the EN 319 403 standard by an accredited body.

6.9 Evidence file

For signatures, Universign will provide Users with the Data extracted from its event log contributing to establishing proof of the constituent operations of an Electronic Signature, subject to the presentation of the appropriate supporting document.

This Data will be transmitted in the form of a file attesting to the authenticity of said Data and stamped via an Electronic Certificate in Universign's name.

The request for access to Data will be made according to the conditions provided in the Contract Annex "Evidence-file access conditions".

Said file will be transmitted as soon as possible as of the receipt of the appropriate supporting document.

After the termination or expiry of this Contract for any reason, the legal Evidence files will be stored for a duration of 15 years from the date of the Transaction subject to (i) disagreement, (ii) inspection, or (iii) judicial requisition.

Article 7 – CONSERVATION SERVICE

The Conservation Service makes it possible to extend the reliability of Documents forming the subject of Electronic Signature or Electronic Seal beyond their period of technological validity, in accordance with the Preservation Policy which more precisely describes the Service's implementation and organization.

7.1. Access to the Service

Access to the Service is an option included in the Electronic-Signature service provided by Universign.

It requires suitable computer equipment to access the Service and:
- a User Account or;
- an account attributed by a Client as part of its organization when the Service is used via APIs.

By default, the Service is provided to all Clients storing electronically signed Documents with a Universign solution.

It may be disabled upon the Client's request.

7.2. Use of the Service

When electronically signed Documents are stored by Universign, the latter carries out processing via its solution allowing the reliability of the Signatures said Documents contain to be extended beyond their period of technological validity.

The Service therefore includes all elements described in the Preservation Policy within the electronically signed Document.

7.3. Limitations of Use

The Service does not constitute an electronic archiving service, particularly with regard to the NF Z42-013 standard.

7.4. Guarantees and limitations of guarantees

Furthermore, Universign guarantees the provision of a Service compliant with the Preservation Policy.

Universign does not guarantee the Service's suitability for the User's needs. It is the User's responsibly to verify this suitability, in particular by ensuring that the Services, as well as the provisions of the Preservation Policy, meet its own requirements.

The use of the Service outside of these guarantees engages the User's exclusive liability.

7.5. Document Storage

It is the User's responsibility to take any provisions to store electronically signed Documents that have been Preserved, as these Documents are not stored by the Service.

7.6. Data retention

Universign keeps event logs relating to the operation of the Preservation Service for a period of fifteen (15) years.

7.7. Limitation of liability

Universign does not control the content of Documents processed as part of the Services, and as such its liability may not be engaged with regard to the value and/or validity of the content of said Documents, or lack thereof.

Universign's liability may not be engaged for consequences of decisions that may have been taken or actions that may be undertaken based on these Documents for which reliability has been extended beyond the period of technological validity.

7.8. Policies and standards

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

1.3.6.1.4.1.15819.5.8.1	ETSI TS 119 511	PP for conservation via extension of signed documents
1.3.6.1.4.1.15819.7.4.1	ETSI TS 119 511	PPD for conservation via extension of signed documents
1.3.6.1.4.1.15819.5.8.2		Conservation Profile
1.3.6.1.4.1.15819.5.8.3		Conservation-Evidence Policies

These policies are published on the publication Site. They are audited according to the EN 319 403 standard by an accredited body.

<u>Article 8 – ELECTRONIC-SIGNATURE AND SEAL VALIDATION SERVICES</u>

The Signature and Seal validation Service allows a User to validate a Signature and Seal previously carried out.

8.1. Access to the Service

The User may benefit from the Service offered as long as it has:

-Suitable computer equipment to access the Service;
-A valid and personal email address (for which they control access);
-A Universign User Account.

8.2. Service description

The validation process for a Signature in a signed Document or a Seal in a sealed Document is based on the following steps:

<u>Step 1: Import of the signed or sealed Document</u>

Via its User Account, the User imports a previously signed or sealed Document in order to verify its validity.

<u>Step 2: Verification of the signed or sealed Document</u>

For each Signature or Seal contained in a signed or sealed document, the Service verifies that:
- The Certificate on which the signature was based was, at the time of the Signature, a Certificate compliant with the provisions of the eIDAS Regulation;
- The Certificate used was issued by a qualified trust-services provider and was validated at the time of the Signature or Sealing;
- The Signature or Seal's validation data correspond to the data communicated to the User;
- The unique set of data representing the Signatory in the Certificate is correctly provided to the User;
- The Signature or Seal, if qualified, were created via a device for the creation of qualified Electronic Signatures or Seals;

- The integrity of signed or sealed data has not been compromised;

Step 3: Issuance and delivery of the Validation Report

Following analysis of a signed or sealed Document, Universign will issue a Validation Report which is then made available to the User via API once.

8.3. Guarantees and limitations of guarantees

Subject to the Users' respect for the applicable TCU and SCU, Universign ensures the enforceability of the content of Validation Reports created through the service, within the meaning of European regulations.

Furthermore, Universign guarantees the provision of a Service compliant with the Validation Policy.

Universign does not guarantee the Service's suitability for the User's needs. It is the User's responsibly to verify this suitability, in particular by ensuring that the provisions of the Validation Policy meet its own requirements.

The use of the Service outside of these guarantees engages the User's exclusive liability.

8.4. Storage of Validation Reports

Universign only stores Validation Reports generated through the Service, in such a way as to preserve their integrity.

Sealed or signed Documents imported for the needs of the Services are deleted from the servers once the analysis step has been completed.

Universign reserves the right to store signed Validation Reports with a specialist subcontractor.

The Validation Reports and the event logs are stored for seven (7) years after their issuance in accordance with application regulations.

However, it is specified that it is the User's responsibility to take any provisions to retain the Validation Report transmitted thereto after analysis, as this cannot be subsequently re-communicated by Universign.

8.5. Users' obligations

The User also undertakes to verify that the signed or sealed Document subject to validation as part of this Service is indeed that transmitted to Universign.

The Service will carry out not archiving of signed or sealed Documents subject to validation, with this remaining the responsibility of Users.

8.6. Limitation of liability

Universign does not control the content of Documents signed or sealed subject to validation as part of the Service, and as such its liability may not be engaged with regard to the value and/or validity of the content of the Documents, or lack thereof.

Universign cannot be held liable for inappropriate use of the Service.

8.7. Policies and standards

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

1.3.6.1.4.1.15819.5.7.1.1	ETSI TS 119 441	CP Validation service
	ETSI EN 319 102-1	Validation algorithm
	ETSI TS 119 102-2	Format of validation report
1.3.6.1.4.1.15819.7.3.1	ETSI TS 119 441	VPD Signature-validation service
1.3.6.1.4.1.15819.5.7.2.1		VP for qualified signatures and seals
1.3.6.1.4.1.15819.5.7.2.2		VP for all types of signatures or seals (qualified or not)

These policies are published on the Website. They are audited according to the EN 319 403 standard by an accredited body.

8.8. Validation report

After analysis of the signed or sealed Document that the User wishes to validate via the Service, a Validation Report is issued by Universign.
For each Signature/Seal present in the Document, it contains the following information:

- the overall validation status of each Signature/Seal;
- the Signature/Seal's ID (in the form of a hash);
- the constraints applied during validation with a status (indicating the success of the verification carried out or any errors encountered);
- the date and time of validation.

The Validation Report will be transmitted in the form of a file attesting to the authenticity of the data it contains and stamped via an Electronic Certificate in Universign's name.

ANNEX 1: EVIDENCE-FILE ACCESS CONDITIONS

1. CONCEPTS

1.1. Transaction evidence file

The elements collected by Universign during a Transaction carried out through the Electronic-Signature service are stored in a file known as the "evidence file".

These elements contribute to demonstrating the reliability of the document-signature process forming the subject of the Transaction.

In particular, the evidence file contains nominative data regarding the Signatory(/ies) and the Collection creator, the digital fingerprint of the signed documents, the email address of Signatories, the email address of the Collection creator, and the telephone numbers to which confidential codes allowing authentication have been sent, as well as the connection addresses (IP) of Signatories (i.e., IP addresses of the devices from which the Signatory accessed the document).

The evidence file is sealed using an electronic seal whose certificate has been issued in the name of *Universign Evidence Service*. It is electronically timestamped shortly after the Transaction, then conserved so as to guarantee its integrity.

With the delivery of this file, Universign attests to the performance of the Signature-related operations registered therein.

1.2. Origin of evidence-file data

The evidence file is made up of data collected directly and indirectly from Signatories.

The data collected indirectly comes from the signature-collection creator.

The other data is collected by Universign directly from the Signatory. The proof of connections, computer records, and other Identification elements (such as the telephone number used for the Signatory's authentication) is established as and when necessary based on the connection logs held by Universign.

1.3. Connection data

This data is generated or processed by the Universign Service during the implementation of the Signature procedure.
Connection data is intrinsically linked to the Transaction but does not form part of its content. This is purely descriptive data which contains the technical elements necessary for the proper functioning of the Signature service.

This data is also subject to regulations regarding the protection of personal data.

1.4. Evidence

The evidence file contributes to demonstrating the existence of a legal deed.

On the one hand, the legal deed is evidenced via a written document which, if drawn up on an electronic medium, must make it possible to identify the person from which it emanates and have been established and stored in conditions guaranteeing its integrity.

On the other hand, in the case of private deeds, the only formal obligation is that they be signed by the parties.

As such, a Transaction evidence file as provided by Universign offers evidence:

- Of the legal deed;
- Of the formal obligation of the electronic signature of a deed to which it relates.

2. EVIDENCE-FILE ACCESS CONDITIONS

2.1. Events permitting access to the evidence file

✓ **Disagreement**

The disagreement opening the right to access to the evidence file is a dispute involving one or more parties to the Transaction or the User Parties. This necessarily concerns the validity of the legal deed from a formal point of view.

Disagreement must arise before a legal procedure.
Disagreement covers, in particular, the amicable settlement of the dispute, mediation and conciliation, whether conventional or legal.

✓ **Legal procedure**

As part of judicial proceedings, an action has been engaged by one of the parties to the Transaction or a Third Party before a competent court to hear the dispute between them.

✓ **Administrative-authority request or inspection**

An imperative request from a supervisory or control authority will give right to access to the evidence file(s), without the need to inform the Signatories concerned by the Transaction or Transactions under inspection in advance.

✓ **Legal requisition**

Some public authorities are legally authorized to have the information contained within the evidence file held by Universign communicated, under certain conditions and as part of their specific missions, without giving prior notice to any of the people involved in the Transaction.

2.2. Persons authorized to access the evidence file

The Persons authorized to access the evidence file differ according to the event giving right to this access.

✓ In case of disagreement or legal procedure:
- The Signatory user(s);
- The collector user(s);
- The User Party(ies).

✓ As part of an imperative request from a supervisory or control authority:
- The empowered authority;
- The collector user(s);
- The User Party(ies).

✓ As part of a Client internal audit:
- The collector user(s).

✓ As part of legal requisition:
- The empowered authority;
- The public prosecutor;
- The investigating judge;
- The judicial-police officer authorized by the public prosecutor.

2.3. Evidence-file access request

The request for access to the evidence file must be addressed to Universign by the authorized Person. Requests must be written and signed by the authorized Person.

Universign requires that person submitting the request to fill in and mail a specific evidence-file access-request form. An original copy of the form must be delivered to Universign by mail.

When the request comes from a public authority, the person submitting the request must justify their authorization.

The request must mention the reason for access: disagreement, administrative inspection, legal procedure or requisition. It is accompanied by the appropriate supporting document, a list of which is indicated in the evidence-file access-request form.

2.4. Term

The evidence file will be transmitted within a period of three (3) working days as of the receipt of the appropriate supporting document.
The request for access to the evidence file is possible for fifteen (15) years after the date of the Transaction forming the subject of the request for access to the evidence file. After this period, evidence files are automatically deleted.