Specific Conditions of Use of Services

The purpose of the present Specific Conditions of Use (hereinafter "**Specific Conditions of Use**" or "**CSU"**) is to define the conditions specifically applicable to the various services offered by Cryptolog International, SAS with capital of €883,527, located at 5-7, rue du Faubourg Poissonnière, 75009 Paris, RCS de Paris n° 439 129 164 (hereinafter "**Universign**").

DEFINITIONS

Unless otherwise stated, capitalized terms have the meaning attributed to them in this article and may be used in the singular or plural, depending on the context.

Certification Authority (CA): refers to the authority in charge of creating, issuing, managing and revoking Certificates in accordance with the Certification Policy.

Preservation Authority (PA): refers to the authority in charge of preserving Electronic Signatures, in particular by means of checks on these elements and methods for extending the reliability of Signatures beyond their technological validity period.

Validation Authority (VA): refers to the authority responsible for validating Signatures and Seals in accordance with the Validation Policy.

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

Electronic Seal: refers to the process used to guarantee the integrity of a sealed Document and to identify the origin of this Document by means of the Certificate used for its sealing.

Electronic Certificate or Certificate: refers to an Electronic Document issued by the Certification Authority containing 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 Certificate holder.

Qualified Certificate: means a Certificate meeting the requirements of Article 28 or 38 of European Regulation n°910/2014 of July 23, 2014.

Customer: means a natural or legal person (i) who has subscribed to the General Terms and Conditions of Sale - Saas, or (ii) who has signed a separate commercial agreement with Universign.

User Account or Account: refers to the computer resources allocated to the User by Universign, enabling him/her to access the Service.

General Conditions of Use (GCU): refers to the general conditions of use applicable to all Services provided by Universign. They are available on the Website.

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

Preservation: refers to the associated service consisting of the implementation of procedures and technologies enabling the reliability of Electronic Signatures or Electronic Stamps to be extended for a specified period.

Time marker: designates a structure that links a Document to a particular moment in time, establishing proof that it existed at that moment.

Electronic Document or Document: refers to all structured data that can be processed by the Service.

Documentation: means the functional and technical documentation provided by Universign in connection with the use of the Services.

Registration file: refers to the file on which the Certificate application is based, containing the information and supporting documents required by the Certification Policy.

Time-Stamping: refers to a process that allows the attestation, by means of Time-Stamps, that a Document existed at a given time.

Authorized Persons: refers to the natural person responsible for the life cycle of the Electronic Stamp Certificate. This is a legal representative of the Subscriber or a person duly authorized for this purpose by a legal representative of the Subscriber.

Third Party: means any individual or legal entity wishing, for its own purposes, to rely on a Certificate or Time Stamp issued by a Certification Authority or to verify the validity of such Certificates or Time Stamps.

Platform: refers to the technical infrastructure comprising all hardware, software packages, operating system, database and environment managed by Universign or its subcontractors, on which the Software Package will be operated. It enables the Service to be provided in SaaS mode. It is directly accessible remotely via the Internet directly on the Website, or using a smartphone or touch-sensitive tablet.

Certification Policy (CP): refers to the set of rules, identified by a number (OID), defining the requirements to which a CA conforms in setting up and providing its services.

Preservation Policy (PP): refers to the set of rules with which the HA complies to implement the Preservation Service.

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

Time-Stamping Policy or TSP means the set of rules with which the TSA complies for the implementation of the Time-Stamping Service.

Subscriber: designates the person, physical or moral, identified in the Certificate who has under his control the private key corresponding to the public key.

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

eIDAS Regulation: means Regulation No. 910/2014/EU on electronic identification and trust services for electronic transactions in 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 by connecting to the shared Platform hosted on the servers of Universign and its subcontractors.

Electronic Seal or Sealing: refers to a process that guarantees the integrity of the sealed Document and identifies its origin by means of the Certificate used for sealing.

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

Signatory: means the natural person who wishes to enter into or has entered into a Transaction with the Customer using the Service.

Electronic Signature or Signature: refers to a process used to guarantee the integrity of the signed Document and to express the consent of the Signatory it identifies.

Website: refers to the www.universign.com website

Storage: refers to the service associated with the Universign Electronic Signature Service, consisting of the possibility of storing Documents signed using the Service on the Platform.

Transaction: refers to the process between the Customer and a third party during which an Electronic Document proposed by the Customer using the Service is signed or time-stamped.

User: refers to a user of the Services, who may be, depending on the case, a Customer, its employees or subcontractors, as well as a third-party Signatory required to use the Services as part of their provision by a Customer.

ARTICLE 1 - PURPOSE

These Specific Terms of Use, together with the General Terms of Use, define the conditions applicable to the Services.

ARTICLE 2 - CONTRACTUAL DOCUMENTS

The CSU form an indivisible whole with the GCU. In any event, they take precedence over any general terms and conditions of purchase of the Customer.

Universign reserves the right to modify the present CSU at any time and without prior notice.

The applicable CSU and previous versions are permanently accessible on the Website, in a format that enables them to be printed and/or downloaded by the User.

ARTICLE 3 - TIME-STAMPING SERVICE

The Service enables Documents to be time-stamped by means of Time-Stamps issued in accordance with the Time-Stamping Policy, which describes in greater detail the implementation and organization of the Service.

3.1. Service access

The Signatory can benefit from the proposed Service on condition that it has :

- Suitable computer equipment to access the Service;

- A User Account.

Use of the Service via the API requires configuration of the User's information system in accordance with the Documentation.

3.2. Use of the Service

The User sends the Document to be time-stamped to the Service, via the Universign API, in accordance with the Documentation.

In response to the User's request, the Service sends a Time-Stamp, the components of which are described in the Time-Stamping Policy.

3.3. Service description

The Service shall not be used to establish proof that an e-mail has been transmitted to or received by a recipient. The Service does not constitute an electronic registered mail service. The Service may not be used for the purpose of identifying the author or origin of the Document.

3.4 Warranties and warranty limits

Subject to the User's compliance with the applicable GCU and CSU, Universign guarantees the enforceability, within the meaning of European regulations, of Time Marks created using the Service.

The Time-Stamping performed using the Service benefits from a presumption of the accuracy of the date and time contained in the Time-Stamp and of the integrity of the Document to which this Time-Stamp relates.

The Time-Stamping Service is synchronized with Coordinated Universal Time so that the accuracy of Time-Stamps is one (1) second.

In the event of an event affecting the security of the Service and which could have an impact on Time Marks, appropriate information will be made available to Users via the Website.

Universign does not guarantee the suitability of the Service for the User's needs. It is the User's responsibility to verify this suitability, in particular by ensuring that the provisions of the Time-Stamping Policy meet their own requirements.

3.5. Obligation of the User

The User undertakes to verify the validity of Time-Stamps as soon as they are received, in accordance with the verification procedure described in the Time-Stamping Policy.

The information required to implement the Time-Stamp verification procedure described in the Time-Stamping Policy is available on the Website.

Apart from the cases provided for in the Time-Stamping Policy, Time-Stamps may be verified for a period of five (5) years from the date of issue.

The User also undertakes to check that the time-stamped Document is indeed the one sent to Universign for time-stamping.

The archiving of Time Marks is the sole responsibility of the User.

3.6. Data retention

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

3.7. Policies and standards

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

OID	ETSI TECHNICAL STANDARD	POLICY
1.3.6.1.4.1.15819.5.1.1	ETSI EN 319 411-1	Time-Stamping Authority PC
1.3.6.1.4.1.15819.5.2.2	ETSI EN 319 421	Time-Stamping Policy

These Policies are published on the Website. They are audited by an accredited body in accordance with standard EN 319 403.

ARTICLE 4 - ELECTRONIC SEAL SERVICE

The Service enables the implementation of two categories of Electronic Stamp whose legal effects are recognized by the regulations applicable within the European Union.

4.1. - Service access

Access to the Service requires :

- Suitable hardware and software to access the Service;

- A User Account ;

- A Certificate of a legal entity associated with cryptographic keys that comply with one of the Certification Policies mentioned herein.

Access to the Service using the API requires configuration of the User's information system in accordance with the Documentation.

Documentation is provided by Universign upon request of the User after the creation of his Account.

4.2. - Use of the Service

The User sends 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 sends the Document on which an Electronic Seal has been affixed.

4.3. - Limits of use

The Service enables an Electronic Seal to be affixed to a Document. It must not be used to establish proof of the consent of the Subscriber 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 Electronic seal categories

4.4.1. Level 1 electronic stamp

Category 1 Electronic Stamps are created using Certificates that comply with the requirements of the ETSI EN 319 411-1 standard, which notably provides for the possibility of remote verification of the Subscriber's identification data.

4.4.2 Level 2 electronic stamp

Category 2 Electronic Stamps are created using Qualified Certificates that comply with the requirements of ETSI EN 319 411-2, which stipulates that the Subscriber's credentials must be verified in the presence of his or her expressly authorized representative.

4.5. Guarantees and limits of Guarantees

Subject to the User's compliance with the applicable GCU and CSU, Universign guarantees the enforceability, within the meaning of European regulations, of Electronic Stamps created using the Service.

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

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

4.6. - Obligations of the User

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

The archiving of sealed Documents is the sole responsibility of the User.

4.7. Data retention

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

4.8. Policies and standards

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

OID	ETSI TECHNICAL STANDARD	POLICY
1.3.6.1.4.1.15819.5.1.3.4	ETSI EN 319 411-1	PC for legal entity certificates, LCP level
1.3.6.1.4.1.15819.5.1.3.5	ETSI EN 319 411-2	PC for legal entity certificates, level QCP-l

These policies are published on the website. They are audited by an accredited body in accordance with standard EN 319 403.

ARTICLE 5 - CRYPTOGRAPHIC KEY SERVICE

5.1. - Service access

Access to the Service requires :

- Creating a User Account ;

- A means of personal authentication accepted by Universign (e.g. a personally assigned cell phone number);

- Subscription to the Certification Service.

The conditions for issuing, managing and revoking Certificates are set out in the Certification Policy.

5.2. - Use of the Service

For the creation of an Electronic Signature, the Bi-Key associated with the Certificate is activated remotely after authentication of the Subscriber by means of a confidential code sent to the telephone number registered with Universign.

To create an Electronic Seal, the Bi-Key associated with the Certificate is activated remotely after authentication of the Subscriber or an Authorized Person using a unique identifier.

Use of the Half-Key by Authorized Persons is deemed to be use by the Subscriber.

5.3. - Limits of use

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

5.4. - Obligations of the User

The User undertakes to ensure the security of his means of authentication so as to prevent the use of the BiKey by unauthorized third parties.

In particular, he/she undertakes to take the necessary measures to guarantee the confidentiality of the means of activation transmitted by Universign and to implement measures to keep the Bi-Key under the exclusive control of Authorized Persons.

5.5. - Universign's obligations

Universign undertakes to generate and activate the Subscriber's Half-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 Subscriber to keep the BiKey under his exclusive control in order to create Electronic Signatures.

The Cryptographic Key Management Service enables the Subscriber and Authorized Persons to keep the BiKey under their control in order to create Electronic Seals.

Universign protects the Bi-Clé's private key to guarantee its integrity and confidentiality.

Universign ensures by appropriate means that the Bi-Key can no longer be used after the Certificate has expired or been revoked.

With the exception of the warranties expressly provided for in the Agreement, Universign excludes all other warranties, express or implied, in particular any implied warranty of fitness for a specific purpose or satisfaction of the Subscriber's requirements.

5.6. - Responsibilities

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

5.7. - Intellectual property rights

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

5.8. - Data retention

Universign keeps the data relating to the control of the User's identification data and the event logs linked to the use of the Bi-Key are kept under conditions that comply with the personal data protection policy available on the Website.

ARTICLE 6 - ELECTRONIC SIGNATURE SERVICE

The Electronic Signature Service provides the Signatory with a solution for creating an Electronic Signature and enables the Customer to collect it.

6.1. Provisions applicable to the Signatory

6.1.1. Service access

The Signatory can benefit from the proposed Service on condition that it has :

- Suitable computer equipment to access the Service;

- A valid, personal e-mail address (access to which is controlled by the customer);

- A means of personal authentication accepted by Universign (e.g. a personally assigned cell phone number).

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

6.1.2. Creating a Universign account

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

As an exception, level 1 Electronic Signature does not require the Signatory to create a User Account.

6.1.3. Service description

The Electronic Document Signature process is based on the following steps:

Step 1: Document availability

The Customer, via his User Account, makes the Document to be signed and, if necessary, adds a Document to be read, available to the Signatory.

Step 2: Invitation to sign

The Signatory is invited to sign the Document via the Service. Where appropriate, an e-mail containing a hyperlink to the Service is sent to the Signatory.

Step 3: Document access

The Signatory is directed to an interface displaying the Document to be signed. The Signatory is invited to read the entire Document.

Step 4: Consent to the Document and CSU/CGU

The Signatory declares that he/she has read the Document and, where the Signature is required, approves its content. The Signatory also declares that he accepts the present CSU completed with the GCU, thus acknowledging the validity and enforceability of the Electronic Signature.

The Signatory's acceptance is materialized by clicking on 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 sent to the telephone number he has declared to Universign or to the Customer. On receipt of the authentication code, the Signatory authenticates himself by entering this code to create the Electronic Signature of the Document.

The Signatory is informed and accepts that the conditions under which his Electronic Signature is collected are satisfactory to produce legal effects and that his Electronic Signature may be validly used against him.

6.1.4. Limits of use

The Signatory undertakes to carry out the steps constituting the Electronic Signature in accordance with the GTU and CSU. Delegation of these operations, delegation of signature and signature to order are prohibited.

6.2. Provisions applicable to the Customer

6.2.1. Service access

Access to and use of the Service by the Customer requires the creation of a User Account.

6.2.2. Service description

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

The Electronic Document Signature process is based on the following steps:

Step 1: Document availability

Through his User Account, the Customer makes the Document available to the Signatory for signing and, where applicable, reading.

Step 2: Invitation to sign

The Customer completes the Signatory data required by the Service.

Step 3: Access to the signed document

Access to the original signed Document is available via the Customer's User account.

6.2.3. Limits of use

The Customer undertakes not to misuse the functionality of the Service or the Signatory's means of authentication, in particular by entering information relating to the Signatory which he knows to be incorrect or by not allowing the Signatory to correctly view the Document to be signed or by entering the confidential code sent to the Signatory himself.

Any use of the Service that does not comply with the GCU and CSU is liable to render the Electronic Signature unenforceable and/or invalidate the document to which it is affixed.

6.3. Electronic Signature Levels

The Service enables the implementation of three levels of Electronic Signature, the legal effects of which are recognized by the regulations applicable in the territory of the European Union.

6.3.1. Level 1 electronic signature

When implementing the Level 1 Signature, Universign cannot guarantee the identity of the Signatory or his credentials. Signatory identification is the responsibility of the Customer, using its own organizational and technical processes, which it implements under its sole responsibility.

Universign authenticates the Signatory by means of the Signatory's telephone number declared to Universign (by the Signatory himself or by the Customer), where applicable.

Level 1 Electronic Signature does not require the Signatory to create a Universign account.

When using this Signature, Universign cannot guarantee the identity of the Signatory, the only elements provided being those communicated by the Customer.

The identification data appearing on the Electronic Signature are those transmitted by the Customer to Universign.

6.3.2. Level 2 electronic signature

As part of the implementation of the level 2 Electronic Signature, the Signatory's identification is checked remotely by means of the digital copy of his identity document sent to Universign.

Universign authenticates the Signatory by means of the Signatory's telephone number declared to Universign (by the Signatory himself or by the Customer), where applicable.

When using this Signature, Universign cannot guarantee the identity of the Signatory. Consequently, it is the Customer's sole responsibility to verify the identity of the Signatory.

Universign checks that the identification data declared is consistent with the proof of identity, a copy of which has been sent to Universign.

Level 2 Electronic Signature is performed using Certificates that comply with the requirements of ETSI EN 319 411-1.

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 his presence and by means of proof of identity.

Universign authenticates the Signatory by means of the Signatory's telephone number declared to Universign (by the Signatory himself or by the Customer), where applicable.

Level 3 Electronic Signature is performed using Qualified Certificates that comply with the requirements of ETSI EN 319 411-2.

6.4. Warranties and warranty limits

As part of the implementation of the Level 3 Electronic Signature, Universign guarantees the use of a Qualified Certificate, the issue of which is subject to verification of the Signatory's identity by appropriate means and in compliance with French law.

Subject to Users' compliance with the applicable GCU and CSU, Universign guarantees the enforceability, within the meaning of European regulations, of Electronic Signatures created using the Service.

Universign in no way verifies that the Service corresponds to the legal regimes applicable to the Documents. Consequently, the provision of the Service does not exempt Users from analysis and verification of applicable legal and/or regulatory requirements.

6.5. Document storage

Unless otherwise specified by the Customer, Universign stores the Documents signed using the Service in such a way as to preserve their integrity. Storage allows the Customer to consult the signed Documents online, to keep them, to return them and/or to destroy them.

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

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

Where Storage is carried out by Universign and unless otherwise agreed between Universign and the Customer, the Documents are stored from the time they are deposited until the occurrence of one of the following events:

- Fifteen (15) years after the filing date of the Document ;

- Closure of the User Account;

- Two (2) months after the end of a Contract unless extended by a reversibility period.

It is the User's responsibility to take all necessary steps to ensure that Documents that are no longer or not at all stored by the Service are preserved in a way that is both durable and honest.

6.6 User obligations

6.6.1. Customer's obligation

The Customer undertakes to:

- That the content of the Documents is lawful and does not permit illegal acts or acts contrary to applicable laws and regulations;

- That the content of the Documents does not infringe the privacy of individuals and/or the provisions relating to the protection of personal data and/or competition law and/or consumer law.

- Where applicable, if the Customer is acting in a commercial or professional capacity, that it complies with the obligations incumbent upon it in respect of its status, particularly in terms of mandatory information and the transmission of signed Documents.

Use of the Service outside these guarantees is the sole responsibility of the Customer.

6.6.2. - Obligations of the Signatory

The Signatory undertakes to :

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

- Ensure the confidentiality of the user ID and confidential code(s) sent to him/her.

6.7. Limitation of liability

Universign does not control the content of the Documents, and therefore cannot be held liable for the value and/or validity of the content of the Documents or for any defect therein.

Universign cannot be held responsible for the consequences of any decisions made or actions taken on the basis of these Documents (whether signed or not).

Universign cannot be held responsible 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 set out in the following table.

OID	ETSI TECHNICAL STANDARD	POLICY

1.3.6.1.4.1.15819.5.1.3.3	ETSI EN 319 411-1	PC for LCP-level certificates for natural persons
1.3.6.1.4.1.15819.5.1.3.1	ETSI EN 319-411-2	PC for certificates of natural persons, level QCP-l

These policies are published on the Publication Site. They are audited in accordance with EN 319 403 by an accredited body.

6.9 Proof file

For signatures, Universign will provide Users with the Data extracted from its event logs to help establish proof of the operations constituting an Electronic Signature, subject to the production of one or other of the appropriate supporting elements.

Such Data will be transmitted in the form of a file attesting to the authenticity of such Data and sealed by means of an Electronic Certificate in the name of Universign.

The request for access to its Data shall be formalized in accordance with the conditions set out in the Appendix "Conditions for access to the evidence file" of the Contract.

The said file will be sent as soon as possible after receipt of the appropriate proof.

After termination or expiration of this Agreement for any reason whatsoever, the Court Evidence Files will be stored for a period of 15 years from the date of the Transaction which is the subject of (i) the dispute, (ii) the review or (iii) the court order.

Article 7 - CONSERVATION SERVICE

The Preservation Service makes it possible to extend the reliability of Documents that have been the subject of an Electronic Signature or an Electronic Seal beyond their technological validity period, in accordance with the Preservation Policy, which describes in greater detail the implementation and organization of the Service.

7.1. Service access

Access to the Service is an option integrated into the Electronic Signature service provided by Universign.

To access the Service, you must have suitable computer equipment:

- a User Account or ;

- an account assigned by a Customer as part of his organization when the Service is used via APIs.

The Service is provided by default to all Customers storing electronically signed Documents with a Universign solution.

It can be deactivated at the Customer's request.

7.2. Use of the Service

When electronically signed documents are stored at Universign, the latter uses its solution to process them in such a way as to ensure the reliability of the signatures they contain beyond their technological validity period.

The Service then integrates all the elements described in the Preservation Policy into the electronically signed Document.

7.3. Limits of use

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

7.4. Warranties and warranty limits

Universign also guarantees to provide a Service that complies with the Preservation Policy.

Universign does not guarantee the suitability of the Service for the User's needs. It is the User's responsibility to verify this suitability, in particular by ensuring that the Services and the provisions of the Preservation Policy meet his or her own requirements.

Use of the Service outside these guarantees is the sole responsibility of the User.

7.5. Document storage

It is the User's responsibility to take all necessary steps to store 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 Conservation Service for a period of fifteen (15) years.

7.7. Limitation of liability

Universign does not control the content of the Documents processed within the framework of the Services, and therefore cannot be held liable for the value and/or validity of the content of the said Documents or for any defect in the latter.

Universign cannot be held liable for the consequences of any decisions made or actions taken on the basis of these Documents, the reliability of which has been extended beyond the period of technological validity.

7.8. Policies and standards

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

OID	ETSI TECHNICAL STANDARD	POLICY
1.3.6.1.4.1.15819.5.8.1	ETSI TS 119,511	PP for extension storage of signed documents
1.3.6.1.4.1.15819.7.4.1	ETSI TS 119,511	PLR for extension storage 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		Proof of Preservation Policies

These policies are published on the Publication Site. They are audited in accordance with EN 319 403 by an accredited body.

Article 8 - SIGNATURE VALIDATION SERVICES AND ELECTRONIC STAMPING

The Signature and Seal Validation Service enables a User to validate a previously operated Signature or Seal.

8.1. Service access

The User may benefit from the proposed Service provided he has :

-Suitable computer equipment to access the Service;

-A valid, personal e-mail address (access to which is controlled by the customer);

-a Universign user account.

8.2. Service description

The validation process for a Signature in a Signed Document or a Stamp in a Stamped Document is based on the following steps:

Step 1: Importing the signed or sealed document

The User, via his User Account, imports a Document that has already been signed or sealed in order to check its validity.

Step 2: Checking the signed or sealed document

For each Signature or Seal contained in a signed or sealed document, the Service checks that :

-The Certificate on which the signature is based was, at the time of the Signature, a Certificate that complied with the provisions of the eIDAS Regulation;

- The certificate used was issued by a qualified trust service provider and was valid at the time of signing or sealing;

- The Signature or Seal validation data corresponds 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, has been created by a qualified Electronic Signature or Seal creation device;

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

Step 3: Issuing and sending the Validation Report

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

8.3. Warranties and warranty limits

Subject to Users' compliance with the applicable GCU and CSU, Universign guarantees the enforceability, within the meaning of European regulations, of the content of Validation Reports created using the Service.

Universign also guarantees to provide a Service that complies with the Validation Policy.

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

Use of the Service outside these guarantees is the sole responsibility of the User.

8.4. Storing validation reports

Universign stores, in a way that preserves their integrity, only the Validation Reports generated using the Service.

Sealed or signed documents imported for Services purposes are deleted from the servers once the item analysis stage has been completed.

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

Validation reports and event logs are stored for seven (7) years from the date of issue, in accordance with applicable regulations.

However, it is the User's responsibility to ensure that the Validation Report sent to him/her after the analysis is kept in a safe place, as Universign will not be able to communicate it at a later date.

8.5. Obligations of Users

The User also undertakes to check that the signed or sealed Document submitted for validation as part of the Service is indeed the one sent to Universign.

The Service does not archive signed or sealed Documents submitted for validation, which remains the responsibility of Users.

8.6. Limitation of liability

Universign does not control the content of the signed or sealed Documents submitted for validation as part of the Service, and therefore cannot be held liable for the value and/or validity of the content of the Documents or for any defect therein.

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

8.7. Policies and standards

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

OID	ETSI TECHNICAL STANDARD	POLICY
1.3.6.1.4.1.15819.5.7.1.1	ETSI TS 119 441	PC Validation service
	ETSI EN 319 102-1	Validation algorithm
	ETSI TS 119 102-2	Validation report format
1.3.6.1.4.1.15819.7.3.1	ETSI TS 119 441	DPV Signature Validation Service
1.3.6.1.4.1.15819.5.7.2.1		PV for qualified signatures and stamps
1.3.6.1.4.1.15819.5.7.2.2		PV for all types of signatures or stamps (qualified or not)

These policies are published on the website. They are audited by an accredited body in accordance with standard EN 319 403.

8.8. Validation report

After analysis of the signed or sealed Document that the User has wished to validate using the Service, a Validation Report is issued by Universign.

It contains the following information for each Signature / Seal present in the Document:

- the overall validation status of each signature/stamp;

- Signature/Stamp identifier (in the form of a hash) ;

- constraints applied during validation with a status (indicating the success of the verification 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 sealed by means of an Electronic Certificate in the name of Universign.

APPENDIX 1: CONDITIONS OF ACCESS TO THE EVIDENCE FILE

1. **NOTIONS**

1.1 Transaction proof file

The elements collected by Universign during a Transaction carried out using the Electronic Signature service are recorded in a file known as the "proof file".

These elements help to demonstrate the reliability of the process for signing the document that is the subject of the Transaction.

The evidence file contains, in particular, nominative data relating to the Signatory(ies) and Collection creator, the digital fingerprint of signed documents, the Signatories' e-mail addresses, the e-mail address of the Collection creator, the telephone numbers to which confidential codes enabling authentication have been sent, and the Signatories' connection addresses (IP) (i.e.: IP addresses of the terminals from which the Signatory accessed the document).

The evidence file is sealed with an electronic seal whose certificate has been issued in the name of *Universign Evidence Service*. It is electronically time-stamped within a short time of the Transaction, and then stored in such a way as to guarantee its integrity.

By transmitting this file, Universign attests to the completion of the Signature operations recorded in it.

1.2 Proof file data origin

The evidence file consists of data collected directly and indirectly from Signatories.

Indirectly collected data originates from the creator of the signature collection.

Other data is collected by Universign directly from the Signatory. Proof of connections, computer records and other elements of Identification (such as the telephone number used to authenticate the Signatory) is established as necessary in support of the connection logs kept by Universign.

1.3. Connection data

These data are generated or processed by the Universign Service when the Signature process is implemented.

Connection data is intrinsically linked to the Transaction, but does not constitute its content. It is purely descriptive data, containing the technical elements necessary for the proper functioning of the Signature service.

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

1.4. Proof

The evidence file helps to demonstrate the existence of a legal act.

On the one hand, a legal act is evidenced by a written document which, if it is drawn up on an electronic medium, must make it possible to identify the person from whom it emanates and be drawn up and stored in conditions that guarantee its integrity.

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

As a result, the Transaction evidence file, as provided by Universign, provides evidence:

- The legal act ;
- The formal obligation to electronically sign a document to which it relates.

2. CONDITIONS OF ACCESS TO THE EVIDENCE FILE

2.1. Events enabling access to the proof file

- **Dispute**

The dispute giving entitlement to access to the evidence file is a dispute involving one or more of the parties to the Transaction or Relying Parties. It necessarily concerns the formal validity of the legal act.

A dispute necessarily arises before legal proceedings are initiated.

Litigation covers, in particular, amicable dispute resolution, mediation and conciliation, whether conventional or judicial.

- **Legal proceedings**

In the context of legal proceedings, an action has been brought by one or other of the parties to the Transaction or by a Third Party before a court having jurisdiction to hear the dispute between them.

- **Request or control by an administrative authority**

An imperative request from a supervisory or control authority entitles the Signatory to access the evidence file(s), without the need to inform the Signatories concerned by the Transaction(s) under control.

- **Judicial requisition**

Certain public authorities are legally authorized to obtain, under certain conditions and in the context of their specific missions, information from the evidence file held by Universign without prior notification of any of the persons concerned by the Transaction.

2.2. Persons authorized to access the evidence file

Persons authorized to access evidence files vary according to the event giving rise to the right of access.

- In the event of a dispute or legal proceedings :
- User(s) Signatory(ies) ;
- Collecting user(s) ;
- The Relying Party(ies).

- In response to an imperative request from a supervisory or regulatory authority:
- Authorized authority ;
- Collecting user(s) ;
- The User Party or Parties.
- As part of a customer's internal audit :
- Collector user(s).
- As part of a judicial requisition :
- Authorized authority :
- The Public Prosecutor ;
- Examining magistrate;
- The judicial police officer authorized by the Public Prosecutor.

2.3. Request for access to the evidence file

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

Universign requires the applicant to complete and send a specific form requesting access to the evidence file. An original copy of the form must be sent to Universign by post.

When the request comes from a public authority, the applicant must provide proof of his or her authorization.

The request specifies the reason for access: litigation, administrative control, legal proceedings or requisition. It must be accompanied by the appropriate supporting documents, a list of which appears on the evidence file access request form.

2.4. Duration

The proof file will be sent within three (3) working days of receipt of the appropriate proof.

A request for access to the evidence file may be made for a period of fifteen (15) years from the date of the Transaction which is the subject of the request for access to the evidence file. At the end of this period, the evidence files are automatically deleted.