GENERAL TERMS OF SUBSCRIPTION TO THE OTU ELECTRONIC SIGNATURE SERVICE AND/OR THE ELECTRONIC SEAL SERVICE

PURPOSE

A. The purpose of this document is to specify the General Terms of Subscription to the electronic Signature service and/or the electronic Seal service which Worldline (formerly known as Atos Worldline) provides for its Subscribers.

B. These Subscribers are:

- either Organizations acting for themselves or on behalf of other Organizations that mandated them to authenticate the origin of the documents issued and guarantee their integrity through the issuance of a Certificate (Organization Certificate or electronic Seal) in the name of their Organization;
- or Subscribers who sign a Contract with Worldline to obtain Certificates:
  - on behalf of their customers so the latter can sign documents electronically (one-time-use Certificates for performing OTU signatures);
  - on behalf of organizations that are contractually associated with them and which mandated them on behalf of their own customers so the latter can sign documents electronically (one-time-use Certificates for performing OTU signatures).

Moreover, these Subscribers can rely on Partners who are contractually affiliated with them to distribute the Subscriber's offerings to the Partners' own customers. In this context, the Subscribers are mandated by the Partners' own customers to obtain, on their behalf, the issuance of one-time-use Certificates that enables them to perform an OTU signature on documents.

C. The distribution and management of Certificates, regardless of their type (one-time-use Certificates or Organization Certificates), are governed by the Certification Policy - Certification Practice Statement, which is under the responsibility of Worldline's OTU Certification Authority.

This CP-CPS is referenced using a public identifier structured as follows:

(OID): 1.2.250.1.111.y.r.v

where:

1.2.250.1 is the high-level OID that identifies AFNOR (*French Standardization Agency*).

111 is Worldline's identifier.

y is the year of creation of the Certification Policy - Certification Practice Statement.

r is the number assigned to the OTU Certification Authority by Worldline. It is based on the year of creation.

v is the major version number of the Certification Policy - Certification Practice Statement.

At time of publication of this document, the OID of the Certification Policy - Certification Practice Statement of the OTU Certification Authority is:

(OID): 1.250.1.111.17.0.3

Versions of the Certification Policy - Certification Practice Statement can be found at https://www.mediacert.com/

D. The Certification Policy - Certification Practice Statement of the OTU Certification Authority has been evaluated by an independent audit firm to validate the compliance with the ETSI standard for the issuance of LCP-level electronic Certificates (LCP: *Lightweight Certificate Policy*). The ETSI standard used for the 2017 compliance audit of the Certification Authority is EN 319 411-1, which, in accordance with European Regulation 910/2014, is the one recommended for the maintenance of the LCP-level Certification.

1. DEFINITIONS

The following terms have the following meanings:

Authentication: electronic process that confirms the electronic identification of a natural or legal person, or the origin and integrity of electronic data. In short, "Identifying yourself is giving your identity. Authenticating yourself is proving your identity." (*French Network and Information Security Agency*)

Authorized representative: refers to any person who is entitled to legally represent a Subscriber company or an Organization. Evidence of this authorization must be provided to the Registration Authority.

Certificate: Electronic file issued by Worldline.

As per the eIDAS Regulation:

- In the case of an "electronic Signature Certificate", this term refers to an electronic Certificate that associates the validation data of an electronic Signature with a natural person and confirms at least this person's name or pseudonym.
- In the case of an "electronic Seal Certificate", this term refers to an electronic Certificate that associates the validation data of an electronic Seal with a legal person and confirms this person's name.

A one-time-use Certificate is a Certificate that is generated dynamically during an online signing process. The platform uses this Certificate during a single signing session after which the signature key is destroyed. Its life span is limited to a few minutes in accordance with the applicable CP-CPS. This Certificate is generated at the Subscriber's request to sign a document at an end user's request.

In the case of one-time use Certificates, the Certification Authority, by signing the Certificate, validates the link between the natural's person identity and the key pair.

The electronic Seal Certificate guarantees the origin of a message issued by a legal person but is also used to encrypt exchanges to ensure their confidentiality, authentication and integrity. In this context, the Organization seals the document in its name as identified in the Certificate, or in the name of the authorized representative of the Organization identified in the Certificate. Organization Certificates are requested by an authorized representative of the Organization.

This electronic Seal or Organization Certificate has a life span of several years in accordance with the applicable Certification Policy - Certification Practice Statement of the OTU Certification Authority.

These Certificates are signed by Worldline's OTU Certification Authority.

Certificate Holder Mechanism: software component that obtains one or more holder Certificates from the Certification Authority and

Subscriber's

guarantees that only the Subject of the Certificate keeps exclusive control over the key pairs. These Certificates are used for electronic Signature purposes, according to the applications and types of Certificates.

Certificate renewal: operation that consists in generating and providing a new Certificate for a Subject. The OTU Certification Authority does not allow for the renewal of one-time-use Certificates.

Certificate Request: the Subscriber who wishes to request an electronic Seal or Organization Certificate must fill in a document included in the Subscription File that notably specifies the contact information of the person(s) who request(s) these Certificates issued by the OTU Certification Authority.

The Subscriber's request for a one-time-use Certificate is an electronic one and consists of a message (request) signed by the Subscriber and kept by the Certification Authority as justification of this request.

Certificate Revocation List (CRL): list of the serial numbers of the Certificates that have been revoked. Its URL can be viewed in Worldline's Certificate.

Certification Authority (CA): authority in charge of implementing the Certification Policy that governs the two types of Certificates i.e. Organization Certificates and one-time-use Certificates. This term also refers to the technical entity that issues the Certificates at the Registration Authority's request. It is responsible for the Certificates signed in its name and carries out the following tasks:

- make sure that the Registration Authority acting on behalf of the OTU CA complies with this CP-CPS;
- publish the public information listed in section 2. 2 of this document, notably the General Terms of Subscription and the Terms of Service, in a durable, secure way;
- guarantee the compliance with the Information Systems Security Policy of the OTU PKI by the various components thereof;
- make its services available to any Subscriber that has accepted the General Terms of Subscription;
- collaborate with auditors during compliance audits and implement any actions that might be decided upon with these auditors following these audits.

Certification Policy - Certification Practice Statement (CP-CPS): set of rules identified by a name (OID) that define the obligations that the CA meets when setting up and providing its services; and which indicate whether a Certificate is applicable to a specific community and/or a category of applications with common security requirements.

The CP-CPS provides an organizational description of Worldline's provision of Certificates, including the process for issuing, using and revoking them.

The CP-CPS is available online at https://www.mediacert.com/

Its reference is *OTU PC-DPC 0002*.

Contractual documents: all the documents listed in section 22 of the General Terms of Subscription.

Conventional Affiliates: Partners or Organizations that are bound by Contract with the Subscriber so they can meet obligations which the Subscriber is in charge of—notably the implementation and compliance with the identification policy defined by the Subscriber beforehand—in exchange for their access, through the Subscriber, to the one-time-use Certificate issuance service provided by the OTU CA. Conventional Affiliates must be expressly mandated by the future Subjects to be able to request a Certificate from the Subscriber on their behalf. They can also be appointed as beneficiaries as per this document.

Document: static electronic document in PDF format.

Electronic identification: the process of using electronic personal identification data that unequivocally represent a natural person, a legal person, or a natural person representing a legal person.

Electronic identification method: material and/or intangible element containing personal identification data and used as an authentication method for an online service.

Electronic Seal: process used by an application service, which makes it different from the "electronic Signature", which is a term reserved for natural persons. "Electronic Seal" refers to electronic data that are logically attached to or associated with other electronic data to guarantee the latter's origin and integrity. It contains a timestamp that corresponds to the date and time on which the Seal was produced.

Electronic Signature: in France, as per the first sentence of paragraph 2 of article 1367 of the French Civil Code below:

The use of a reliable identification process guaranteeing its link with the document which it is associated with.

As per Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, "electronic Signature" means *data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign*.

In the context of this document, the electronic Signature does not constitute a qualified signature.

When an Organization Certificate or electronic Seal is used, it is not a natural person's electronic Signature. The possible use of the term "electronic Seal signature" must be understood as the use of a Seal that guarantees the origin and integrity of a message.

Electronic timestamping: electronic data that associate other electronic data with a specific instant and proves that the associated data existed at that instant.

End user: refers to a natural-person signatory who has carried out a transaction with the Subscriber, or the Partners or Organizations contractually affiliated with the Subscriber, and who uses the service provided by the latter. The end user is the Subject of a one-time-use Certificate.

The end user can benefit from the services provided they meet the following prerequisites:

- have the legal capacity to make commitments in accordance with the provisions applicable to the use of the service;
- possess valid, up-to-date identity documents so they can identify themselves;
- possibly have an e-mail address or a telephone number for certain services, in which case, this information must be active, accurate and personal.

Evidence: as opposed to proof (legal concept), the term "evidence" refers to data and documents that are intended to establish proof. It may notably include computer traces, timestamping files, electronically signed files, or any other document or file that the Subscriber can use to demonstrate the existence and validity of the transaction carried out.

Evidence Management Policy: document that describes the policy which the CA implements to constitute and keep the evidence of the electronic exchanges that took place. The Evidence Management Principles describe the rules, processes and context related to the establishment and retention of Evidence as part of dematerialized services. They explain the security properties that should be achieved (integrity, authenticity, etc.) and how to achieve them (in particular through the electronic Signature, timestamping, computer traces, among others).

Identification: act of establishing the identity of a natural or legal person, or of a natural person representing a legal person. This process notably relies on verified, valid legal credentials.

Journey: functional process that results in the OTU signing of one or more documents. A Subscriber can define multiple journeys. Journeys are to be differentiated in particular when the Subject

Subscriber's initials

identification conditions are different, requiring the definition and validation by the Registration Authority of distinct *OTU Identification Policy and Consent Collection Methods* documents.

Online Certificate Status Protocol (OCSP): online Certificate verification protocol that makes it possible to verify the status of an X.509 digital Certificate.

Organization: entity that notably represents a company, a public Administration, etc. or which can refer to the name of a brand or company for which an Organization Certificate will be delivered at a Subscriber's request.

OTU Identification Policy and Consent Collection Methods: two-part document drawn up by the Subscriber from the *OTU FORM 0018* form to back up one-time-use Certificate requests:

- The first part describes the Subject or end user identification processes that the Subscriber implements or whose implementation is contractually delegated, under the Subscriber's responsibility. The Registration Authority approves the identification policy after verifying its compliance with the requirements described in paragraph 3.2.3.1 *Validation of the identity of a one-time-use Certificate Subject* of the CP-CPS.

- The second part details the process by which the Subscriber, directly or through its Conventional Affiliates, collects the end user's explicit, informed consent before requesting any one-time-use Certificate on behalf of the end user. It notably specifies the actions that must be carried out before the issuance of the OTU Certificate so the Subject can agree with the implemented process, give their consent to the document presented to them and sign it electronically.

Parties: Worldline and the Subscriber.

Party: Worldline or the Subscriber.

PDF: computer file format created by ADOBE Systems®. Its particularity is that it preserves the formatting defined by the author.

Personal identification data: set of data used to establish the identity of a natural or legal person, or of a natural person representing a legal person;

Private key: authentication, signature or encryption key that the Certificate Holder Mechanism shall keep secret and which is associated with a Public key contained in a Certificate.

Registration Authority (RA): authority in charge of receiving the Subscriber's Certificate requests, verifying them in accordance with the checks described in the CA's Certification Policy based on the type of Certificate requested, archiving them, and sending them to the CA. The RA is also in charge of receiving and processing Certificate Revocation requests.

As per this document, Worldline is responsible for the RA. Worldline thus relies on the Subscriber's commitment to verifying identities, directly or through its Conventional Affiliates. These verifications are described in the Subscriber's identification policy(ies) and may vary according to the contexts in which one-time-user Certificates are issued.

The issuance of a one-time-use Certificate requires that the Subscriber, directly or through its Conventional Affiliates, has previously identified the persons who request such Certificates in accordance with the mechanism described in a document called *OTU Identification Policy and Consent Collection Methods* provided by the CA as a form, and which it undertakes to fill in and abide by. Such a document will be drawn up for each journey of the same Subscriber whose identification and/or consent conditions differ.

Before its implementation, the document entitled *OTU Identification Policy and Consent Collection Methods* described by the Subscriber must have been accepted by the CA and the RA during the subscription request or the implementation of a new journey.

The identification policy complies with the rules described in section 3.2 *Initial identity validation* of the OTU CA's CP-CPS, and sets out the verifications that the Subscriber will implement, directly or through the agents or Partners with whom it is contractually bound, in order to provide a process for the reliable identification of its customers (Subjects).

The RA performs sampling-based checks with the Subscriber, including its Conventional Affiliates, to check the compliance of the identification mechanism described by the Subscriber.

Registration file: forms and supporting documents that enable the CA to justify the issuance and/or use of electronic Certificates to perform signatures or electronic Seals on behalf of the Subscriber.

Revocation: operation requested by the Certificate Holder Mechanism, the Subscriber's representative, a Subscriber's deputy representative who has the identification and authentication data required to access this function, or the OTU CA (in accordance with the OTU CA's CP-CPS) to invalidate a given Certificate before the end of its validity period. The Certificate may become invalid for many reasons other than natural expiry, such as the loss or compromise of the private key associated with the Certificate, or a change in at least one field included in the name of the Subject/possessor of the Certificate. The revocation operation is considered as finished when the serial number of the Certificate to revoke and the revocation date are published in the CRL. The revocation of the Certificate has no consequences on the validity of the documents signed or sealed with this it during the period that precedes its revocation.

Service: certification service provided by Worldline for the Subscriber to meet the latter's needs in terms of electronic signing of PDF documents.

Service activity logs: all OTU service application logs (Certificate and signature/Seal production).

Signatory: natural person who creates an electronic Signature.

Subject: natural or legal person identified in the Certificate as its possessor.

In the case of a one-time-use Certificate, the Subject is a customer of the Subscriber or of the Conventional Affiliates authorized by Subjects to mandate the Subscriber to request a Certificate on their behalf.

When the Certificate is an Organization Certificate, the Subject is the Organization or a representative thereof. Therefore, the generation and exclusive use of the private key associated with the public key specified in the Certificate is entrusted to the "Certificate Holder Mechanism" entity.

Subscriber: refers to the company that signs the Subscription Contract, has subscribed to the Certificate delivery service provided by the OTU CA, and wants to obtain, as it chooses, the delivery of

- Organization Certificates on behalf of Organizations that depend on the Subscriber or on behalf of Organizations that expressly mandate the Subscriber for this purpose;

- one-time-use Certificates in the name of the Subjects that it will have identified beforehand or the identification of whom will have been contractually delegated to Conventional Affiliates, under its own responsibility.

Subscriber's beneficiary: a person who holds a right because of its link, be it contractual or legal, with the Subscriber.

Subscription Contract: refers to the Contract by which one subscribes to the electronic Signature Service and/or electronic Seal service. It consists of the documents referred to in Article 22, which form an inseparable whole.

Trust chain: set of Certificates required to validate the filiation of a Certificate delivered to an entity. The OTU CA's trust chain consists of its Certificate as well as the Certificate of the MediaCert root CA.

Website: Worldline website dedicated to the services.

Working day: every day of the week except Saturday, Sunday and public holidays.

Subscriber's initials

2. PREREQUISITES TO THE ESTABLISHMENT OF THE SUBSCRIBER STATUS

2.1. The acceptance of the Subscriber status is based on a set of elements defined in chapter 3.2.2.1 V*alidation of a Subscriber* of the OTU CA's CP-CPS. This notably includes

- the signature of a Subscription Contract,
- the designation or appointment of Representatives within the Subscriber for the one-time-use and/or Organization Certificate creation requests, and
- a set of supporting documents.

2.2. In the event where an Organization is different from the Subscriber, the latter must provide the RA with the information concerning the Organization as defined in paragraph 3.2.2.2 *Validation of an Organization* of the OTU CA's CP-CPS.

2.3. The signature of the Subscription Contract constitutes recognition, particularly by the Subscriber, of the obligations contained in clause 8 of this document and in the OTU CA's CP-CPS.

3. CONDITIONS TO BE MET BEFORE CERTIFICATES CAN BE OBTAINED

To obtain Certificates, the Subscriber shall do the following:

3.1. The Subscriber must make its Certificate Creation Request (ref. *OTU FORM 0007*) in accordance with the service which it has subscribed to with the CA, depending on whether it is an Organization Certificate (or electronic Seal) and/or a one-time use Certificate.

3.2. The Subscriber is responsible for ensuring that the Certificates and/or the chosen level of electronic Signature are adequate for its needs and those of its possible Conventional Affiliates. Before making any Certificate creation to the RA, the Subscriber is responsible for making sure that the type of the Certificate to be delivered as part of the service is adapted to its internal delegation rules, its business needs, its legal constraints as well as those of its Conventional Affiliates.

4. DELIVERY OF AN ORGANIZATION CERTIFICATE

4.1. **Subscriber File**

The Subscriber File sent to the electronic Seal service that uses Organization Certificates must be completed with supporting documents as described in paragraph 3.2.2.2 *Validation of an Organization* of the CP-CPS.

The RA may reject any incomplete file. The information supplied in the file must be complete, accurate and up to date. The Subscriber guarantees that it has verified the information provided and the validity of the supporting documents that come with it. Any modification of the information contained in the file must trigger the procedure for revoking the issued Certificate for any of the following reasons: death, departure or resignation of a Subject of an Organization Certificate. Worldline reserves the right to refuse the file if the Subscriber is insolvent, is being sued, or breaches moral standards in any way whatsoever.

4.2. The Subscriber guarantees the verification of the Subscriber information provided, the validity of the supporting documents that come with it, and the regular updating of such information. Worldline incurs no liability towards the Subscriber concerning the format, accuracy, authenticity or legal effect of the supporting documents supplied by the Subscriber. The electronic Seal or Organization Certificate produced by the CA is sent to the Subscriber via e-mail to be validated before use.

4.3. **Certificate acceptance**

Explicit acceptance of the information contained in the Certificate is required either from the legal representative of the Subscriber that makes the request, or from the individual authorized by the Subscriber's legal representative and identified in the Certificate. The formalism of this acceptance is detailed in the CP-CPS as well as in the e-mail notification of the issuance of the electronic Seal or Organization Certificate sent by the OTU CA.

4.4. The Subscriber shall inform Worldline in writing about any inaccuracy within the seven (7) working days that follow the generation of said Certificate, notably if the data contained in it do not match the information contained in the Subscription File. If no notification is sent within that time, or if the Subject has used the Certificate, the latter will be considered as accepted. If a notification is sent during the aforementioned time frame, Worldline will provide the Organization with a new Certificate.

4.5. The validity period of an electronic Seal Certificate or Organization Certificate is defined in the CP-CPS and in clause 1 of this document.

4.6. Two (2) months before the expiry date of the Organization Certificate, a notification is sent to the Subscriber to invite it to request a new Organization Certificate. In the absence of a new request from the Subscriber, the service is interrupted when the Certificate expires.

4.7. The new Certificate is imperatively generated with a change of private key.

5. DELIVERY OF A ONE-TIME-USE CERTIFICATE

5.1. **Subscriber File**

The Subscriber File sent to the signature service that uses one-time-use Certificates must be completed by supporting documents as described in 3.2.3.1 *Validation of the identity of a one-time-use Certificate Subject* of the CP-CPS.

In particular, it must contain the Identification Policy and Consent Collection Methods document.

The Subscriber that requests the issuance of one-time-use Certificates must, in accordance with the applicable CP-CPS, implement or have implemented, the processes—recognized by the RA— used for the reliable identification of the future Subjects of such Certificates. These processes must have been described beforehand in the aforementioned document. The Subscriber guarantees the verification of the information provided and the validity of the supporting documents that come with it. Worldline incurs no liability towards the Subscriber concerning the format, accuracy, authenticity or legal effect of the supporting documents supplied by the Subscriber and the Subject(s).

Any file whose identification policy does not include the verifications required for the reliable identification of customers, who are the future Subjects of Certificates of this type, will be refused by the RA.

5.2. **Certificate Request**

In the case of one-time-use Certificates, the Subscriber's electronic message sent to the CA to request a Certificate must include the information described in section 4.1.2.1 *Processes and responsibilities when establishing a Certificate request* of the CP-CPS, and it must be signed electronically by the Subscriber.

5.3. The Subscriber recognizes that the Certificate that will be issued at its request on the Subject's behalf will contain the following verified information about the Subject's identity: forename, surname, and date and place of birth.

6. USE OF AN ORGANIZATION CERTIFICATE

6.1. The use of such Certificates must comply with the applicable CP-CPS. Indeed, the Subscriber undertakes to use the Certificates issued by the CA exclusively for the applications that allow the use of an Organization Certificate as described in section 1.5 *Use of Certificates* of the CP-CPS. Worldline may not be held liable if this obligation is breached.

6.2. For electronic Seals or Organization Certificates, the Subscriber authorizes the CA to use the private key associated with the Certificate for the purpose of implementing electronic Seals.

6.3. Before use, the user must check, at least, the information on the status of the Certificate that they intend to use in accordance with the intended use. This can be done by using the various available methods in accordance with paragraph 4.9.10 of the applicable CP-CPS.

Subscriber's initials

7. USE OF A ONE-TIME-USE CERTIFICATE

7.1. The use of such Certificates must comply with the applicable CP-CPS. Indeed the Subscriber undertakes to use the Certificates issued by the CA exclusively for applications that allow the use of a one-time-use Certificate as described in section 1.5 *Use of Certificates* of the CP-CPS. Worldline may not be held liable if this obligation is breached.

7.2. The Subscriber, including its Conventional Affiliates, recognizes that the electronic Signature process implemented must be presented clearly to the end user. The latter must be able to accept it before it is implemented and, on this occasion, to mandate the Subscriber so the latter can request a one-time Certificate on their behalf so they can sign the document(s) presented to them.

8. REVOCATION OF ORGANIZATION CERTIFICATES

8.1. **Origin of the revocation**

The authorized persons or entities are described in paragraph 4.9.2.2 *Origin of a revocation request - Organization Certificates* of the CP-CPS.

8.2. **Cause of the revocation**

The causes of revocation are described in paragraph 4.9.1.2 *Possible reasons for a revocation - Organization Certificates* of the CP-CPS.

8.3. **Liability**

Worldline can in no way be held liable if an authorized representative of the Subscriber has not sent a Certificate revocation request when one of the circumstances described in the aforementioned paragraph of the OTU CA's CP/CPS, and which they are aware of, occurs.

8.4. **Revocation procedures**

The procedures for processing a revocation request are described in paragraph 4.9.3.2 *Processing of a revocation request - Organization Certificates* of the CP-CPS.

The revocation of an Organization Certificate results in the generation of a CRL. The number of the Certificate that is the subject of the revocation request is added to the CRL.

The OTU CA then publishes this CRL at the address defined in paragraph 4.10 *Certificate status information function* of the CP-CPS.

The users of such Certificates can view this list without any limitation.

8.5. **Confirmation of the revocation**

As part of a request for the revocation of such Certificates, Worldline will send an e-mail to the requisitioner to confirm the execution of the Certificate revocation request.

9. REVOCATION OF ONE-TIME CERTIFICATES

9.1. **Origin of the revocation**

The authorized persons or entities are described in paragraph 4.9.2.1 *Origin of a revocation request - One-time-use Certificates* of the CP-CPS.

9.2. **Cause of the revocation**

The causes of revocation are described in paragraph 4.9.1.1 *Possible reasons for a revocation - One-time-use Certificates* of the CP-CPS.

9.3. **Liability**

Worldline can in no way be held liable if an authorized representative of the Subscriber has not sent a Certificate revocation request when one of the circumstances described in the aforementioned paragraph of the OTU CA's CP/CPS, and which they are aware of, occurs.

9.4. **Revocation procedures**

The procedures for processing a revocation request are described in paragraph 4.9.3.1 *Processing of a revocation request - One-time-use Certificate* of the CP-CPS.

The revocation of any Certificate results in the generation of a CRL. The number of the Certificate that is the subject of the revocation request is added to the CRL.

The OTU CA then publishes this CRL at the address defined in paragraph 4.10 *Certificate status information function* of the CP-CPS.

The users of such Certificate can view this list without limitation.

9.5. **Confirmation of the revocation**

Since the revocation request is automatically authorized, the Subject concerned is informed of the change of status of their Certificate by the publication of the CRL at the addresses defined above.

10. SUBSCRIBER'S OBLIGATIONS

10.1. **Provision of documents for the RA by the Subscriber**

Electronic Seal or Organization Certificates

The Subscriber must provide the RA with

- the document by which it requests the creation of an electronic Seal Certificate or Organization Seal, filled in by an authorized Subscriber representative if it wishes to create such a Certificate;
- the supporting documents that back up the content of the Certificate that the CA will produce; and
- in particular, if the name of the Organization to be put in the Certificate differs from that of the Subscriber:
    - a valid supporting document (mandate) from the legal or authorized representative of the Organization in question allowing the Subscriber to request the delivery of a Certificate on behalf of that Organization; and
    - all the supporting documents necessary to substantiate the powers of the representative of this Organization if the natural person who represents the Organization is not the legal representative thereof (valid, non-revoked delegation of power); and evidence that this natural person is part of this Organization.

The Subscriber shall verify the validity and completeness of the documents which it provides the CA with at the time of its subscription request.

One-time-use Certificates

The Subscriber must provide the RA, which will have to validate it, with the *Identification Policy and Consent Collection Methods* document that it or its beneficiaries will have completed with its assistance and under its responsibility.

This document contains

- a written description of the process for identifying one-time-use Certificate Subjects. It is imperative that this identification process include the presentation of an identity document or a copy of an identity document of a Subject; and verifications attesting to the validity of this document, performed before or during the electronic Signature process.
- The consent collection methods process must describe the process that enables the Subscriber to obtain the end user's explicit, informed consent to certain things prior to any one-time-use Certificate request on their behalf.
- The points subjected to the Subject's consent notably include

Subscriber's initials

- the Subject's consent to give the Subscriber the necessary power so the latter can initiate a request to the OTU CA to obtain a Certificate on the Subject's behalf; and
- the Subject's explicit agreement for the CA to collect and process their data for the purpose of providing the Subject with an electronic Certificate; and to keep these data in order to meet its obligations vis-à-vis Auditors.

10.2. **General obligation of the Subscriber to inform Subjects**

The Subscriber shall inform the end user, in its capacity as Subject, about the clauses of its Subscription Contract. Consequently, the Subscriber shall also provide, prior to any action from the end user, the information that they need to in order to understand the terms of the online contracting process, notably

- by informing them about the process through which they express their consent, the electronic Signature process used, and by setting out the legal consequences of their various actions;
- by informing them about the content of the evidence created, and by telling them who is charge of managing and preserving this evidence:
- by informing them that they can abort the procedure that they have initiated;
- by telling them whether they may withdraw or not;
- by informing them about the conditions under which the contractual document that they have signed can be made available to them, and how this document is preserved; and
- by inviting them to read the Terms of Service of the OTU PKI, which are available online at https://www.mediacert.com/

10.3. **Verification of the content of Certificate creation requests**

The Subscriber shall verify the accuracy and completeness of the information supplied to the RA in the signed electronic message (request) on in the paper-based form intended for the RA, and which is required for the issuance by the OTU CA of either a one-time-use Certificate or an Organization Certificate.

10.4. **Non-discriminatory practices**

The Subscriber also undertakes not to have any discriminatory practices as part of the services that it delivers and which could be detrimental to those provided by the OTU CA.

10.5. **One-time-use Certificate Subjects' compliance with their Obligations**

Moreover, the Subscriber shall make Subjects comply with the clauses of the Subscription Contract that are applicable to them.

To this end, it will see to ensure Conventional Affiliates' compliance with these clauses vis-à-vis the Subjects.

The Certificate must be used in accordance with the clauses of the CP-CPS in force.

10.6. **Information of the RA by the Subscriber**

Electronic Seal or Organization Certificates

The Subscriber shall

- inform the RA if the Certificate's data become invalid because of a change in the Organization. To do so, the Subscriber must inform the RA immediately, by means of registered mail with acknowledgment of receipt, of
  - any change in the identity of the person who has the role of Subscriber representative or deputy Subscriber representative, the effective date of this change and the supporting documents;
  - any change in the information sent to the RA and the effective date of these changes.
- inform the RA as soon as possible of any event that might affect the reliability of the methods one uses to authenticate oneself with it. In this case, the changes (forename, surname, e-mail address) must be notified to the RA.
- inform the RA should the Organization cease to exist. In this case, the Subscriber must inform the RA immediately, by means of registered mail with acknowledgment of receipt, of the changes (forename, surname, e-mail address, Organization identifier) that affect all of the Organization's Certificates, and must provide the supporting documents.

  and
- inform the RA if the information that concerns the Organization, and which does not appear in the Organization Certificate and has no impact on its validity, is modified. In this case, the Subscriber must inform the RA as soon as possible, through a simple letter, of the changes in the information.

One-time-use Certificates

The Subscriber shall

- inform the RA as early as possible of any event that might be detrimental quality of the identification of its future Subjects; and
- inform the RA as early as possible of any event that might be detrimental to the reliability of the methods that it uses to authenticate itself with said Authority.

11. WORLDLINE'S OBLIGATIONS

11.1. Worldline undertakes to implement the (technical and human) means required for the provision of the services. The level of service provided is the one defined in the Contract referenced in the Subscription Contract enclosed with these General Terms.

11.2. Worldline shall use the generated keys only to produce the electronic Signature(s) needed for the execution of a transaction requested by the Subscriber.

11.3. Through the Certificate Holder Mechanism, Worldline undertakes to use the end user's or the Organization's private key only for the purposes provided for by the OTU CA's CP-CPS.

11.4. Worldline undertakes to authenticate any request from the Subscriber that concerns a Certificate request and undertakes to keep, in particular, evidence of this request.

11.5. Worldline keeps all the data needed by the OTU CA defined in chapter 5.5.2 *Archive Retention Period* of the OTU CA's CP-CPS, including:

- registration files
  - for eight (8) years for one-time-use Certificate registration files;
  - for ten (10) years for Organization Certificate registration files.
- service activity logs for ten (10) years.

11.6. Worldline has a duty of advice vis-à-vis the Subscriber so the latter can choose, in an informed way, the technical electronic Signature solution adapted to the type of signature journey that it has determined. Worldline's intervention is limited, as part a of best-effort obligation, to a technical service that enables the Subscriber or its beneficiaries to benefit from electronic Signature and/or electronic Seal services for documents in accordance with the applicable CP-CPS. Worldline does not act on the content of the documents subjected to the services provided by the OTU CA, except for the insertion of electronic Signatures and/or electronic Seals, not does it access the content of the documents to provide its

Subscriber's initials

services. Worldline may not be held liable for the value or validity of the content of the documents.

12. SERVICE INTERRUPTION

The Subscriber understands that Worldline may have to interrupt all or part of the service to maintain or improve it. Worldline informs the Subscriber as soon as possible of any planned interruption (in particular by e-mail or through information on the Website) and limits the duration of the interruption and its impact on the service.

13. AGREEMENT WITH REGARD TO EVIDENCE

The Parties expressly agree that in the context of their contractual relationships, dated electronic messages are mutual evidence. The Parties agree that when an issuer sends an electronic message to a recipient, the latter is deemed to have received it through the return of the acknowledgment of receipt.

14. FINANCIAL TERMS

The OTU CA does not market its Certificates alone, but only through higher-level services specified in the Contract referenced in the Subscription Contract associated with these General Terms of Subscription.

All financial terms are described in detail in this Contract.

15. SUBSCRIBER'S LIABILITY AND GUARANTEES

Liability

15.1. Vis-à-vis Worldline, the Subscriber is solely liable for the correct execution of the Subject identification and authentication steps, and for the adequacy of the choice of the electronic Signature process for its needs and those of its possible Conventional Affiliates.

15.2. If Worldline is not the recipient of the supporting documents collected by the Subscriber—including those collected by the Conventional Affiliates—to back up the identification of Subjects, Worldline samples some of the one-time-use signatures performed for the Subscriber to make sure the latter, including its Conventional Affiliates, properly implements the Identification Procedure validated jointly by the Parties. This sampling must help make sure that the identity verification has been carried out and requires that the evidence thereof be kept for a minimum of eight (8) years by the Subscriber, including its Conventional Affiliates. This sampling campaign will take place at least once a year. In the event of discrepancies with this procedure, the Subscriber agrees to establish an action plan with Worldline to eliminate them. The non-implementation of this action plan or the observation of discrepancies during the next sampling campaign might result in the deactivation of the electronic Signature service that uses one-time-use Certificates for the Subscriber, including its beneficiaries, in accordance with the provisions of the CP-CPS.

Guarantees

15.3. Moreover, the Subscriber shall hold Worldline harmless against any action, dispute or claim that might be initiated by a Subject or third party, and any resulting damage caused directly or indirectly by the failure of the Subscriber, its beneficiaries or a Subject, to comply with any of the clauses of the Subscription Contract including the related documents.

15.4. Generally, the Subscriber, including its Conventional Affiliates, guarantees the OTU CA that the content of the documents transmitted by it and/or its Conventional Affiliates is lawful and does not make it possible to perform actions that violate the applicable laws and regulations in force.

15.5. The Subscriber is prohibited from making any commitment in the name and on behalf of the OTU PKI, which it may not replace in any case whatsoever.

16. WORLDLINE'S LIABILITY AND GUARANTEES

Liability

16.1. Worldline provides a technical service by providing the Subscriber with the electronic Signature and/or electronic Seal services of the OTU CA.

16.2. The Subscriber acknowledges that the OTU CA does not act on the content of the documents issued by the Subscriber, except for the insertion by the OTU CA of Signatures or electronic Seals into said documents; and that the OTU CA thus cannot be held liable for the content and information that they contain.

16.3. Worldline's liability is limited to direct property damage and excludes any indirect damage. If Worldline's liability is established, it is expressly agreed that Worldline may only be liable for compensation up to an amount that may not exceed the amount specified in the Service Contract, the references of which are specified in the Contract of Subscription to the OTU electronic Signature service and/or electronic Seal service (ref. *CTRA OTU 0005*) enclosed with these General Terms.

16.4. Worldline holds no liability whatsoever for the consequences of delays, alterations or losses that the Subscriber might incur as part of the transmission of any electronic messages, postal mail or documents.

16.5. In accordance with article 12 above, Worldline will not be held liable in the event of a complete or partial interruption of the service.

16.6. The OTU PKI can only be held liable if the failure to comply with its obligations is proved.

16.7. The OTU PKI can in no case whatsoever be held liable in the event of a fault occurring within the scope of a Subscriber entity, and notably

- use of an expired Certificate,
- use of a revoked Certificate, or
- use of a Certificate for a use other than those described in section 4.5 of the CP-CPS.

16.8. Generally, the OTU CA is not liable for the documents and information provided by the Subscriber, and does not guarantee their accuracy or the detrimental consequences of facts, actions, negligence or omissions due to the Subscriber, its representative or the Subject.

16.9. Should Worldline be held liable in its capacity as CA because of a failure of the Subscriber, including all of its beneficiaries, to meet one of the obligations incumbent upon it, the Subscriber will replace Worldline for any settlement of disputes or any resulting legal action coming from a beneficiary, user or third party.

16.10. **Force Majeure**

Worldline cannot be held liable for any loss, damage, delay or failure to meet the obligations resulting from the General Terms when the circumstances that cause them fall under force majeure within the meaning of Article 1148 of the French Civil Code. Moreover, the Parties further agree that the following shall constitute cases of force majeure: decisions of a public authority, legislative and/or regulatory amendments, and unpredictable facts due to a third party that cause damage which render the provision of the service impossible. Should the force majeure situation prevent either Party from meeting its obligations for a period of time exceeding two months, each Party will be allowed to cancel the Subscription Contract as of right and without any legal formalities, in which case the Subscriber will not be able to claim any compensation.

Guarantees

16.11. Worldline guarantees the Subscriber that the services provided comply with the applicable Certification Policy accessible on the MediaCert Website on the day on which the service is used.

16.12. Worldline cannot replace the Subscriber when it comes to choosing the level of service subscribed in accordance with the legal regimes applicable to the Business Documents for which the Subscriber has decided to use the electronic Signature and/or the electronic Seal.

16.13. Consequently, Worldline's provision of the service does not exempt the Subscriber from the analysis and verification of any applicable

Subscriber's initials

legal or regulatory requirements in force relating to the aforementioned Business Documents.

16.14. The OTU CA undertakes to issue Certificates in accordance with the CP-CPS concerned and the state of the art.

16.15. Through its services, the OTU PKI guarantees

- the authentication of the Subscriber by the RA through the Subscriber's Certificate;
- the generation of one or more Certificates in accordance with a Subscriber request authenticated and verified beforehand;
- the provision, by the OTU CA, of functions that provide information about the statuses of the issued Certificates, at the Subscriber's request, in accordance with this document;
- the exclusive control of the private key of the Certificate by the Certificate Holder Mechanism, and the destruction of this key after a one-time-use session in the case of one-time-use Certificates.

17. AMENDMENT OF DOCUMENTS AND CONTRACTUAL CONDITIONS

Documentary changes due to external constraints

17.1. **General Terms of Subscription**

The General Terms of Subscription that are likely to evolve to take into account legal, technical or commercial constraints will be updated.

In this case, Worldline will have to modify or update these General Terms and Conditions by simply updating their content to take these changes into account.

Worldline will specify at the earliest, via a signed e-mail announcement, the updates made to the General Terms of Subscription.

This notification will specify the effective date of said updates.

17.2. **CP-CPS and/or Terms of Service**

In the event of a change affecting the CP-CPS and/or the Terms of Service of the OTU PKI in force, the Subscribers will be informed, via a signed e-mail announcement, one (1) month at the latest before the publication of the new version of the modified document in accordance with the change that affects it.

This notification will specify the effective date of these updates.

17.3. Any notification between the Parties will be validly sent to the Subscriber's e-mail address specified in its registration file or to any other address that the Parties may give each other later via postal or electronic mail.

17.4. In the event of a change likely to have a major impact on the Subscriber and/or Worldline and its Organization, these updates will be notified to the Subscriber in accordance with section 9.11 *Individual notifications and communications between participants* of the CP-CPS.

17.5. Each version of the aforementioned updated documents will be available and accessible online as soon as they come into force at https://www.mediacert.com/

17.6. The Subscriber, including its beneficiaries, is informed of the possibility to save and/or print the applicable General Terms of Subscription.

Documentary changes made by the OTU CA

The changes made to a contractual document will be brought to the Subscriber's attention by any means, at least one (1) month before they come into force.

If the commercial changes made as part of the service were to affect the economy of the Contract referenced in the Subscription Contract, the Subscriber would then be allowed to cancel its Contract in the event of a disagreement, without incurring any penalty. If no cancellation occurs, and if the Subject(s) continue(s) using the Certificate(s) when the aforementioned period of time expires, the Subscriber will be deemed to have accepted said changes.

18. DURATION

The Subscriber's Contract takes effect on the day on which the Subscriber signs it, for an undefined duration which, however, may not exceed the duration of the higher-level Service Contract specified in the Subscription Contract.

19. CANCELLATION

19.1. The Subscriber or the CA may cancel the Subscription Contract as of right and without any legal formalities through registered mail with acknowledgment of receipt:

- for convenience reasons after complying with notice period stipulated in the Contract referenced in the Subscription Contract;
- without notice, if the other Party fails to meet any of its contractual obligations, if such failure has not be remedied by the failing Party within one (1) month following a formal request through registered mail with acknowledgment of receipt (first delivery attempt) that has not been answered;
- in cases of force majeure, under the conditions described in Article 16.10 of this document;
- automatically, in the event of the termination of the Service Contract which this Subscription Contract is associated with.

19.2. In the event of the termination of the Subscription Contract and on the effective date of the termination, access to the service will be deactivated for the Subscriber and its beneficiaries; moreover, Electronic Seal Certificates possibly issued will be immediately revoked without notice and without any possibility for the Subscriber to claim any right to compensation.

19.3. The Subscriber is prohibited from requesting the creation of a Certificate from the RA on the effective date of the termination.

20. INTELLECTUAL PROPERTY

The provision of a Certificate does not give the Subscriber or Subjects any property right over the Certificate.

21. PROTECTION OF PERSONAL DATA

21.1. **Electronic Seal or Organization Certificates**

The personal data collected as part of this Subscription Contract are mandatory for the processing of the registration file. This information, like that which will be collected later, is intended for the OTU PKI which, by express agreement, is allowed to store it using computer memory, use it and transmit it for the same purposes and with the same protection, to the artificial persons of Worldline, or to authorized third Parties for the management of Electronic Seal Certificates.

21.2. **One-time-use Certificates**

In the context of one-time-use Certificates, the Subscriber will see to obtain the express acceptance of future Subjects before transmitting the latter's personal data to the OTU PKI's RA so the latter processes the requests for the creation of such Certificates.

For this purpose, the future Subject will have to accept that their personal data collected by the RA are subjected to computer processing for the sole purpose of meeting the following objectives:

- constitute their identification and allow their authentication so a Certificate can be generated on their behalf;
- be able to give them the activation data of their private key;

Subscriber's initials

- back up the identity specified in the Certificate by providing the necessary evidence, if need be, through the retention of the elements in the registration file.

It must be noted that any opposition to the retention of personal data will prevent the issuance of such Certificates. Indeed, by accepting the delivery of the Certificate to perform an electronic Signature, the Subject accepts that the OTU PKI, through the RA and at the latter's request, keeps the personal data for the duration required by the purposes of the processing operations carried out as part of the delivery and management of one-time-use Certificates.

21.3. The Subscriber, the representatives of Subscribers or Organizations, and Subjects have a right of access, rectification, deletion and opposition concerning the personal data that they have supplied. They can exercise this right by contacting Worldline at the address below:

Comité "MediaCert OTU"
Worldline
1, rue de la Pointe
Zone Industrielle A
59113 Seclin France
dlfr-mediacert-ac-otu@atos.net

21.4. This right of rectification, deletion and opposition must not, however, preclude the right to keep the data that make it possible to establish a right or Contract for as long as required by the purpose for which the data are stored.

21.5. Worldline has implemented and complies with personal data protection procedures to ensure the security of data transmitted by

- the Subscriber including all of its Conventional Affiliates;
- the Subjects, who are natural persons, to the Subscriber—including all of its Conventional Affiliates—which transmits these data to Worldline under this Contract for the purpose of identifying and authenticating these Subjects.

21.6. It is the Subscriber's responsibility to obtain natural-person Subjects' consent to the transmission to the RA and the CA, for computer processing purposes, of the personal data that the Subscriber—including its Conventional Affiliates—collect in order to identify and authenticate Subjects. This is necessary for the RA and the CA to issue Certificates on behalf of Subjects so the latter can sign online the documents presented by the Subscriber.

21.7. The Subjects must guarantee the Subscriber, including its Conventional Affiliates, that the data that they provide for this purpose are accurate. The Subjects must be informed of their right to rectify the information that concerns them if this information is modified.

21.8. The Subjects must be informed of the nature of the information that concerns them, which is kept to prove the electronic exchanges that were carried out, if need be. This information is detailed in the Evidence Management Policy, which can be obtained through an electronic request (e-mail).

The Subscriber, including the Conventional Affiliates or the third party designated by the Subscriber, undertakes to obtain the future Subjects' prior consent to the transmission of their personal data to the RA and the CA, since these data are necessary to justify the issuance of a Certificate in their name, and to prove the electronic exchanges that took place and their accountability.

21.9. The Parties shall comply with the French Data Protection act of 6 January 1978 amended by the Act of 6 August 2004 relative to the protection of personal data. Therefore, each Party shall

- submit to the French Data Protection Authority the declarations related to the protection of its own customer files;
- ensure the security of personal data during their transmission to the other Party regardless of the transmission method used, in accordance with the aforementioned act.

Each Party is fully responsible for its own files and the processing that they undergo.

21.10. The Parties shall abide by the laws that apply to them and guarantee this compliance to each other.

The Parties guarantee that all of their staff, and any other person under their responsibility, will meet the obligations set out in this article.

21.11. The obligations contained in this article are applicable for the duration of this Contract and for an unlimited time after its termination.

21.12. The Parties shall provide each other with any information that is useful for the correct execution of the processed operations, in accordance with the French Personal Data Protection act.

22. CONTRACTUAL DOCUMENTS

22.1. The Subscription Contract consists of the documents listed below, which form an inseparable whole:

- the Contract for Subscribing to the OTU electronic Signature and/or electronic Seal service;
- these General Terms of Subscription to the OTU electronic Signature and/or electronic Seal service; and
- the CP-CPS available online at the address defined in Article 1.

In addition, in the event of the issuance of OTU Certificates, this Contract is supplemented, during the Subscriber's subscription request to Worldline, with the *OTU Identification Policy and Consent Collection Methods* document.

22.2. All the aforementioned documents make up the technical framework in which the electronic Signature service is provided for the Subscriber. It is supplemented by the provisions of the higher-level Service Contract which clarify; in particular; article 14 of this document about financial terms, article 18 about the duration, and article 16 about Worldline's liability.

In the event of a contradiction between the articles of the General Terms of Subscription and those of the provisions of the higher-level Service Contract, the clauses of the General Terms of Subscription, which derive from the applicable CP-CPS, shall prevail.

23. APPLICABLE LAW

The interpretation, validity and execution of this Contract are governed by French law.

All the components of the infrastructure referred to as OTU PKI, including its documentation, are governed by the applicable legislation and regulations in force on the French territory, even though some of the activities deriving from the CP-CPS associated with these General Terms may have legal effects outside of the French territory.

Moreover, only the French versions of the contractual documents listed in article 9 of this document are enforceable against the Parties, even if translations exist. Indeed, translations, by explicit agreement, are provided for convenience only and have no legal effect, notably on the interpretation of the Subscription Contract or of the common intention of the Parties.

24. SETTLEMENT OF DISPUTES

In the event of any dispute concerning the interpretation, formation or execution of this Contract, and if no amicable settlement can be reached, any dispute will be brought before the competent courts of Paris.

CYRIL LOOTVOET

Signature numérique de CYRIL LOOTVOET
Date : 2018.04.12 15:32:04 +02'00'

Subscriber's initials