Document reference	OTU.PC-DPC.0002
Document revision:	3.1
Document date:	21/07/2017
Classification:	Public

OTU Certification Authority

Certification Policy
Certification Practice Statement

CYRIL LOOTVOET

Signature numérique de CYRIL LOOTVOET
Date : 2018.04.12 15:28:29 +02'00'

Change log

Version	Date	Author	Reason
1.0	24/12/2012	C.BRUNET	Initial public release
1.1	08/04/2013	C.BRUNET	Changes following remarks during the initial ETSI 102 042 audit • 4.9.2.1: reworded the origins of the revocation • 5.8.2: clarification of extended CRLs in the event of a cessation of activity
1.2	22/11/2013	C.BRUNET	Changes following a contract adjustment • 3.2.3.1: additional explanations about the retention of data when they are not used in Certificates • 5.5.2: modified the retention periods of registration files • 9.6.4: the term "immediately" is replaced by "as early as possible" • 9.9, 9.13, 9.14, 9.16.5: modified the reference to Client /AWL contracts
1.3	01/02/2015	C.BRUNET	- Changes made because of the company's name change - Modified the Certificate template • Entire document: Atos Worldline is replaced by Worldline (**NB**: this is the same company with the same SIRET registration number.). • 7.1.2.3: modified the values specified in the "DN", "Subject Alt Name" and "Key usage" fields •
2.0	07/11/2016	V. DUMOND C. LOOTVOET A. BRUGNOT J.J. MILHEM	Changes following audit feedback • - Modified paragraph 3.2.3.1 for the validation of the identity of a Subject of a one-time-use Certificate through external identification - for the case where the Subject belongs to the Subscriber's Organization, reworded the obligation to verify the Subject's identity; • added procedures and reasons for destroying the CA's Key Pairs in subsection 6.3.4; • the word "operator" has been replaced by "pilot". • made guarantee limitations consistent with the General Terms of Use (section 9.7); • modified paragraph 4.9.3.2 to describe the procedure for revoking an Organization Certificate; • added the methods that guarantee that the revocation period is complied with (paragraph 4.9.3.2 and subsection 5.7.3); • added subsections 5.2.5 and 5.2.6, and modified subsection 5.3.6 so the CA complies with the requirements set out in subsection 7.4.3; • added subsection 5.4.6 about the procedures for returning and verifying the return of event logs;

			• modified subsection 5.2.4 about the roles requiring remit separation; • added the OIDs of test Certificates (subsection 1.2.2) and added descriptions (paragraphs 7.1.2.4 and 7.1.2.5); • added the OTU CP's OID into all Certificate templates; • added paragraph 4.9.10 about CRL archiving; • added description of the monitoring of the Mediacert page (subsection 2.4.2); • added a reference to the signing of the CA's documents to make sure they have been authenticated (subsection 2.4.3); • revised subsection 5.3.2 about the verification of criminal records; • modified templates and OIDs to keep up with the change of version of the CP (subsection 1.2.2, and paragraphs 7.1.2.2, 7.1.2.3, 7.1.2.4 and 7.1.2.5); • added a sentence to subsection 3.2.4 to indicate that the e-mail address is not verified during the Certificate request; • corrected subsection 7.1.5 about the name constraints that affect the CN attribute, and the GN and SN attributes in the case of Organization Certificates, if applicable; • modified subsection 9.12.2 about the circumstances under which the OID must be changed; • added missing definitions; • rewording and clarifications regarding the contract, the subscription file, the Subscriber's obligations, Subject identification and Organization validation; • added a step of acceptance of the Certificate by the Subject of an OTU Certificate; and • added to section 9.6 a pledge against discriminatory practices.
2.1	02/02/2017	C. LOOTVOET	• Modified the Subject information that must be collected, verified and kept by the CA (paragraph 3.2.3.1) • Revised CRL profiles (section 7.2) • Revised Certificate templates (section 7.1) • Modified the duration of the notice period in the event of a modification of the CP (subsection 9.11)
3.0	6/9/2017	F. LESECQ V. DUMOND	Rewriting to take into account eIDAS regulatory constraints
3.1	7/21/2017	F.LESECQ, F. DA SILVA	Taking into account the remarks of the eIDAS audit

Contents

1 Introduction

1.1 General presentation

This document describes the Certification Policy of the OTU Certification Authority established by Worldline to govern the entire life cycle (creation, issuance, use) of the One-Time-Use (OTU) signing Certificates implemented as part of the OTU online subscription process, but also the life cycle of the electronic Certificates used to seal electronic data to ensure their origin and integrity.

In this context, this document presents

- the requirements which the OTU Certification Authority complies with during the registration and verification stages of Certificate requests,
- the uses for which Certificates are issued,
- the management of these Certificates throughout their life cycles,
- the security measures applicable to the Public Key Infrastructure, and
- the obligations and requirements of the various participants.

In addition to describing the Certification Policy, this document describes the Certification Practice Statement. It states the practices that the OTU Certification Authority uses when managing the Certificates that it issues.

This document is applicable to the Certificates intended for a Certificate Holder Mechanism managed by Worldline. Four (4) types of Certificates are considered, in accordance with subsection 1.2.2 and section 7.1 of this document:

- One-time-use Certificates in accordance with ETSI standard [EN 319 411-1], LCP level;
- Organization Certificates in accordance with ETSI standard [EN 319 411-1], LCP level;
- One-time-use Certificates for test purposes in accordance with ETSI standard [EN 319 411-1], LCP level; and
- Organization Certificates for test purposes in accordance with ETSI standard [EN 319 411-1], LCP level.

1.2 Identification

1.2.1 Document identification

Elements	Value
Title	**Politique de certification - Déclaration des Pratiques de Certification (anglais)**
Document reference	**OTU DPC 0003**
Version	**3.1**
Author	**Worldline**
Product reference	**OTU Certification Authority**

This document will be referred to as "CP/CPS" throughout.

1.2.2 Certification Authority identification

The name of the Certification Authority concerned by this Certification Policy is "OTU".

The OID of this CP/CPS is **1.2.250.1.111.17.0.3**

This OID is based on the OID assigned to Worldline by AFNOR (*French national organization for standardization*) (which is 1.2.250.1.111) and is constructed as follows: 1.2.250.1.111.X.y.z.w where

- *x* is the year of creation of the Certification Policy / Certification Practice Statement. 2017 → 17.
- *y* is the number assigned to the Certification Authority by Worldline based on the year of creation.
- *z* is the version of the Certification Policy / Certificate Practice Statement.
- *w* is the type of the Certificate used by the OTU CA.

As implied by the above description, the OTU CA has defined an OID for each type of Certificate that it issues. These OIDs are

- OID of one-time-use Certificates [LCP]: 1.2.250.1.111.17.0.3.1
- OID of Organization Certificates [LCP]: 1.2.250.1.111.17.0.3.2
- OID of one-time-use Certificates for test purposes [LCP]: 1.2.250.1.111.17.0.3.3
- OID of Organization Certificates for test purposes [LCP]: 1.2.250.1.111.17.0.3.4

The OTU CA is attached to an Atos Worldline Root Certification Authority whose necessary information is as follows:

Elements	Value
***OID* of the Root CP/CPS**	**1.2.250.1.111.12.0.2**
***Distinguish Name* (DN)**	**C = FR** **O = Atos Worldline** **OU = 0002 378901946** **CN = AC Racine – Root CA – 2012**

The OTU PKI's Certification Chain has the following structure:

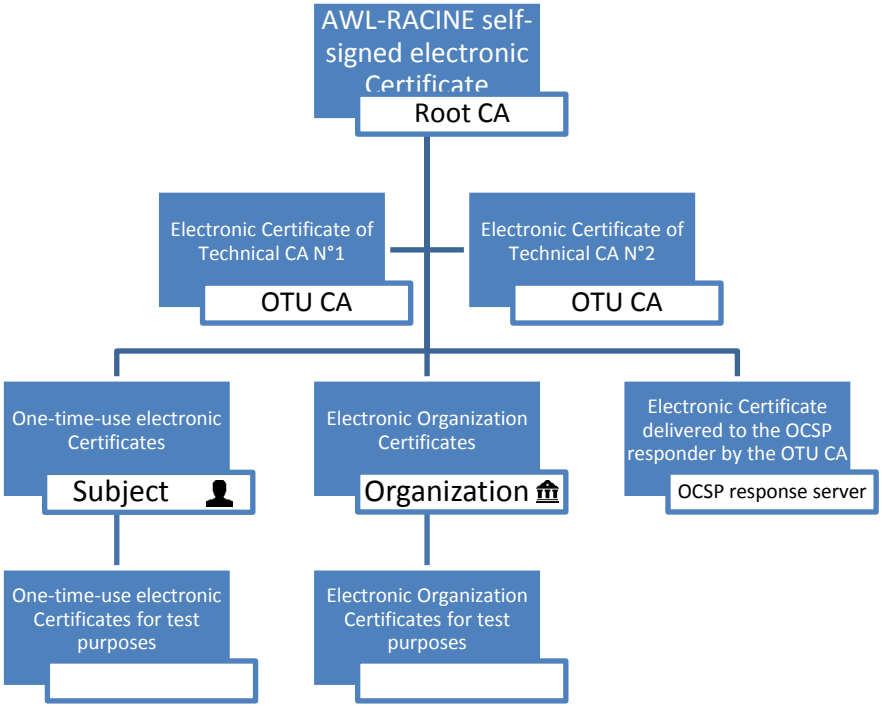

Figure 1 - Certification Chain of the OTU PKI

1.3 Entities involved in the PKI

The Public Key Infrastructure (PKI) consists of a set of technical, human, documentary and contractual resources dedicated to managing the life cycle of the electronic Certificates delivered by the Certification Authority. It provides a secure environment for electronic exchanges by means of asymmetric cryptographic systems.

The OTU CA is based on this technical infrastructure. The services that the PKI provides are the product of various services that correspond to the various stages of the life cycles of Key Pairs and Certificates. For this reason, the OTU PKI consists of a number of entities as presented by the block diagram on figure 2.

In terms of functionalities, the OTU PKI can be broken down as follows:

- Registration authority,
- Certificate generation service,
- Certificate delivery service,
- Certificate revocation service, and
- Certification status information service.

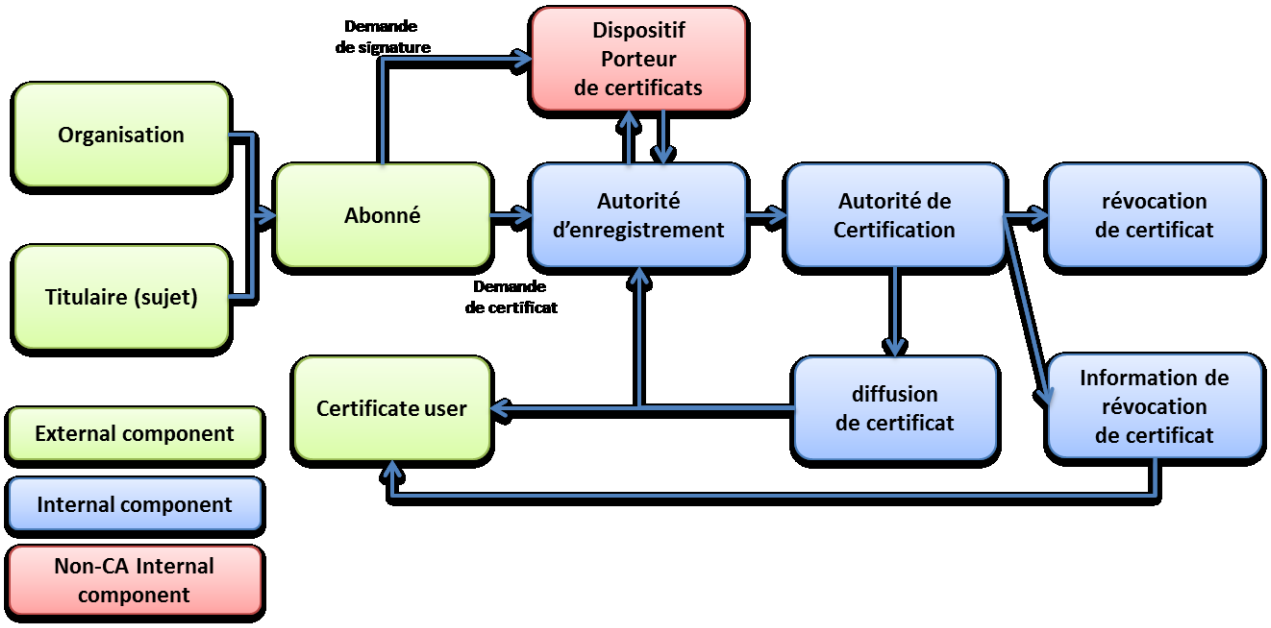

Figure 2 - Block diagram of the OTU PKI

1.3.1 Certification Authority

A Certification Authority (CA) is an entity capable of producing Certificates at the request of the Registration Authority. This entity is in charge of the complete life cycle of Certificates (creation, publication, etc.).

Generation service
This service generates the Certificates from

- the information given by the Registration Authority, and
- the public key of the Certificate created by the function that generates the secret data.

These Certificates are signed electronically with the OTU CA's private key and can only be used for the purposes described in paragraph of this CP/CPS.

Transmission service
Once the Certificates are generated, they are sent to the Registration Authority, which in turn sends them to the Certificate to the Certificate Holder Mechanism.

Revocation service
This service revokes the Certificates from a revocation request that has been submitted beforehand. The results are indicated through the Certificate status information service.

Certificate status information service
This service gives Certificate users information about the statuses of Certificates (revoked, suspended, etc.). This function is implemented through publication channels that are updated regularly i.e. Certificate Revocation Lists (CRLs), the Authority Revocation List (ARL) and the OCSP responder.

The OTU Certification Authority is also represented by an Authority Manager appointed within Worldline. This Authority Manager personally appoints Deputy Authority Managers who report to them.

1.3.2 Registration Authority

The Registration Authority (RA) is the entity that is in contact with customer units (Subscribers), which send it Certificates creation or revocation requests. As such, it performs the following operations:

- authentication of the Subscriber that requests the creation of a Certificate,
- verification of the content of Certificate creation requests,
- registration of Certificate creation or revocation requests,
- acceptance or rejection of Certificate creation or revocation requests,
- delivery of the Certificates to the Certificate Holder Mechanism, and
- archiving of Certificate creation or revocation requests.

To provide these services, the OTU CA operates its own RA. The latter relies on a department that has the technical and human resources required to manage the life cycle of Certificates for the OTU CA. These resources thus constitute a single point of access to this Certification Authority (servers that allow for the transmission of requests and the delivery of Certificates).

1.3.3 Certificate Holder Mechanism

In the context of this CP/CPS, the Certificate Holder Mechanism is different from the Certificate's Subject.

Indeed, the term "Certificate Holder Mechanism" refers to a software and hardware entity that is hosted by Worldline and stores the Certificate and private key of the Subject or an Organization.

For each Certificate generated by the OTU CA, the Certificate Holder Mechanism is responsible for the following tasks:

- generation of the Key Pair,
- secure storage of the Key Pair,
- generation of the Certificate Signing Request (CSR) that contains the user information sent beforehand by the Subscriber,
- use of the private key and the Certificate in the use cases described in section 1.5, and
- destruction of the private key as described in paragraph 6.2.10.2 of this document.

The Certificate Holder Mechanism stores the secret data securely and has exclusive control over them on behalf of the Subject or Organization.

1.3.4 Certificates beneficiaries

The delivery of Certificates by the OTU CA requires prior subscription to the services of this CA. This entails the signing of a Subscription Contract with the OTU CA. This contract specifies the type of Certificate that the Subscriber wants to implement:

- one-time-use (OTU) signing Certificate issued in the name of a natural person so documents can be signed (see paragraph 1.5.1.1), and/or
- electronic Certificate for sealing documents on behalf of its Organization or a principal Organization (see paragraph 1.5.1.1).

OTU signing Certificate

Moreover, it must be noted that in the case of OTU signing Certificates, it is the Subscriber that requests a Certificate from the OTU RA by means of a message that it signs electronically. In this case, the Subscriber

- must, before requesting a Certificate for the Subject, have identified the latter so the Certificate issued can be based on a reliable, reasonably verified identity (see paragraph 3.2.3.1); and
- must have obtained the Subject's consent needed to be able to request the generation of an OTU Certificate from the RA (see paragraph 3.2.3.1).
- The Certification Authority will then produce a one-time-use Certificate (see subsection 1.4.1).

Electronic seal
To seal electronic data on behalf of Organizations that are associated with the Subscriber, legally or through an agreement, the OTU CA produces Organization Certificates (see subsection 1.4.2).
Indeed, the Organization, through the Subscriber, will then use a Certificate operated by Worldline to guarantee the integrity of the documents and authenticate their origin.

An Organization Certificate may refer to the person who represents the Organization legally, statutorily or by agreement. This person is

- either the legal representative appearing in the Organization's company registration certificate ("Extrait Kbis" in French) or
- a person duly authorized—whether statutorily or by agreement—to represent the Organization and appear in the Certificate.

In any case, the competent bodies within the Organization must have duly authorized the appointed person to appear in the Certificate.

The person who has the right to include their identity in the Certificate must prove it to the RA to be able to act as a representative of the Organization. If the Organization is not the Subscriber and allows the Subscriber to act on its behalf, the Subscriber will have to prove to the RA that it has the rights to act on behalf of this Organization. It will also have to prove that the appointed person has the rights to include their identity in the Certificate and to represent the Organization.

The Subscriber's representative is the only person authorized to submit Certificate requests to the RA.

Therefore, a representative of the Subscriber must be designated in writing to the RA. This representative of the Subscriber can be

- the Subscriber's legal representative (as they appear in a company registration certificate of the Subscriber less than three months old);
- its contractual representative (as they appear, for example, in the statutes); or
- a representative authorized by the legal representative to represent the Subscriber as part of the execution of the Subscription Contract.

Although the Subscriber and the Organization are the same entity in most cases, it is possible to differentiate them. For example, a Subscriber may want to use a brand name rather than the name of the subscribing company. Besides, if a group has multiple subsidiaries, the Subscriber and the Organization may have different names.

In any case, the Subscriber will have to prove that it is legally allowed (ownership of the name, company registration certificate, mandate, etc.) to specify an Organization name that differs from its own.

The Subscriber, through its legal or statutory representative, can formally appoint, in writing, one or more deputy Subscriber representatives who are also authorized to represent it. To do so, the Subscriber must inform the RA and give the aforementioned persons the necessary powers.

1.3.5 Certificate users

The user of a Certificate is the natural or legal person that uses the information of a Certificate that it/they receive(s) for the purposes described in paragraph 1.5.1.1. This signature or seal is associated with a document.

It must be noted that the signature of a document is mostly used by the products supplied by ADOBE™, such as Acrobat Reader©. These products have functions for viewing the signature of the document.

Not all other document viewers also include functions for viewing signatures.

It is the users' responsibility to verify the revocation status of the Certificate, at least before using it, using the various means at their disposal as described in subsection 4.9.10.

1.3.6 Other participants

Human resources complete the system:

- computer system operators (in charge of maintaining systems in operational condition), and
- teams in charge of maintaining compliance.

1.4 Types of Certificates

The OTU CA produces four (4) types of Certificates that are notably differentiated by their OIDs (see subsection 1.2.2).

1.4.1 One-time-use Certificates

A one-time-use Certificate is dynamically generated by the OTU CA for a physical person (Subject), at the Subscriber's request, during the electronic signing process.

This Subject may be a natural person acting for their own needs or those of their Organization, on behalf of which they are duly authorized to sign.

This Certificate is used during a single signing session (signing of the various documents of a contract for the Subject) by the Certificate Holder Mechanism. As explained in subsection 6.3.2, it has a very short life span.

The Subscriber sends the one-time-use Certificate request to the OTU RA by means of a message that it signs electronically. This message contains:

- the Subject identification data, and
- an electronic seal that guarantees the integrity of the identification data as well as the Subscriber's identity.

Once the Subscriber's request for a one-time-use Certificate has been verified and validated by the RA, the Certificate is issued by the OTU CA, which signs the Certificate containing the identity of the Subject that appears in the Certificate, said identity having been verified by the Subscriber.

Indeed, the Subscriber is responsible for the identification data that are sent to the RA in the request and which make it possible to create a Certificate that contains the Subject's verified data.

The Subject's private key is generated using a specific secure device in accordance with the information given in paragraph 6.2.1.1 of this document.

Once the one-time-use Certificate has been used for the Subject at the Subscriber's request, the corresponding private key is destroyed in the HSM as described in paragraph 6.2.10.2. The Certificate, however, remains accessible in the signed document.

1.4.2 Organization Certificate

The Organization Certificate is issued following a request made by the Subscriber to Worldline, on behalf of the Organization(s) for which the Subscriber is entitled to request document sealing (in accordance with the use defined in paragraph 1.5.1.1). This service is operated by Worldline on its own premises.

Requests for such Certificates are made in accordance with a procedure that involves an authorized representative of the Subscriber and a registration operator from Worldline. The information that must be provided for the request is detailed in paragraph 4.1.2.2 of this document.

This CP/CPS does not impose any physical presence requirements but reserves the rights to have additional checks performed, such as verification phone calls.

An Organization's private key is generated using a specific secure device in accordance with the information given in paragraph 6.2.1.1 of this document.

1.4.3 Test Certificate

For technical purposes (i.e. testing whether the service is up and running), or for the demonstration and acceptance tests of the changes made to the production information system, the issuance of test Certificates by the production OTU CA is allowed.

Indeed, the Subscriber may request the creation of test Certificates from the RA, for its own use or for a Subject.

Test Certificates may in no way be used to hold the holder, Subscriber or Worldline liable in the same way a production Certificate does. However, the Subject's, Subscriber's and OTU CA's obligations regarding the protection and use of the Certificate are identical to those defined for production Certificates.

For these test Certificates, it is imperative that the *CommonName* attribute of the *Subject* field be prefixed with the word "TEST" (see subsections 7.1.5 and 7.1.6). These Certificates must be revoked as soon as they are no longer needed.

The limitations of use and liability applicable to production Certificates also apply to test Certificates.

1.5 Use of Certificates

1.5.1 Areas of use

1.5.1.1 Key Pairs and Certificates

This CP/CPS concerns the Key Pairs and the associated electronic Certificates that are managed by the Certificate Holder Mechanism (defined in subsection 1.3.3), and which enable electronic Certificate Subjects to

- electronically sign a document with a one-time-use Certificate, and
- electronically seal a document with an Organization Certificate

as part of paperless contracting or transmission processes.

1.5.1.2 Key Pairs, CA Certificates and component Certificates

The OTU CA's Key Pair is used exclusively to sign Certificates and CRLs whose templates are defined in chapter 7 of this document.

Its Certificate is signed by the higher-level Certification Authority as described in subsection 1.2.2 of this document.

1.5.2 Prohibited uses

Any use of a Certificate issued by the OTU CA that violates the uses described in subsection 1.5.1 of this CP/CPS is strictly prohibited. The OTU CA may not be held liable for any such prohibited use.

1.6 CP management

1.6.1 Entity that manages the CP

Worldline is responsible for drawing up this CP/CPS, maintaining it, and revising it as soon as necessary. To this end, a Security Committee is in place within the OTU PKI. It consists of

- at least one representative of the OTU CA,
- the OTU CA's security officer, and
- at least one member of the team in charge of monitoring platform compliance, depending on the documentary validation requirements.

It decides, at least once a year, whether changes should be made to this document and thus verifies its compliance with the state of the art, and with the applicable laws and regulations in force.

1.6.2 Point of contact

The authorized contact for any comment, request for additional information, claim or submission of a litigation file concerning this CP/CPS is

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

1.6.3 Entity that determines whether a CPS complies with this CP

The consistency of the CPS is guaranteed by the uniqueness of this document, and by its review and validation by the Security Committee upon any major modification (see subsection 9.12.1).

1.6.4 CPS compliance approval procedure

Worldline is responsible for the compliance of the practices documented in this CP/CPS. To this end, Worldline relies on the Security Committee (see subsection 1.6.1) whose role is to validate these practices through regular monitoring of the state of the art or following the results of external audits.

The process for verifying the compliance of the CP/CPS is specified in subsection 1.6.3.

The changes made to the CP/CPS are notified to the stakeholders concerned, and the CP/CPS is made available to them immediately.

1.7 Definitions and abbreviations

1.7.1 Key definitions

The definitions of the key technical terms used in this CP are provided below.

Authentication: electronic process that confirms the electronic identification of a natural or legal person, or the origin and integrity of electronic data.

Certificate: standardized X509 data that make it possible to associate a public key with its possessor. A Certificate contains data such as the possessor's identity, their public key, the identity of the organization that issued the Certificate, its validity period, a serial number, a thumbprint or even usage criteria. All these elements are signed by the CA that issued the Certificate.

Certificate Holder Mechanism: software component that obtains one or more Certificates from the CA. These Certificates are used, according to the applications and types of Certificates, for the uses defined in subsection 1.5.1.
The Certificate Holder Mechanism consists of servers and cryptographic boxes operated at the same time as the CA. It guarantees holders the exclusive control of Key Pairs and Certificates.

Certificate Request: request made by the Subscriber to the RA to obtain a Certificate for a natural or legal person related to the Subscriber. This natural or legal person is identified and authenticated beforehand by the Subscriber or by the persons duly authorized for this purpose, under the Subscriber's responsibility. It includes information which the Subscriber must provide the Registration Service with along with the Certificate request.

Certificate template: computer data resulting from the registration of a Subscriber that requests Certificates by the Registration Service. These data are then sent to the Certification Authority to be signed.

Certification Authority (CA): authority in charge enforcing this CP/CPS; the term also refers to the technical entity that produces Certificates at the request of the Registration service, and more broadly manages them (generation, delivery, revocation, publication, logging and archiving) in accordance with this CP/CPS. Further information is provided in subsection 1.3.1.

Certification Chain: set of Certificates necessary to validate the filiation of a Certificate delivered to an entity.

Certification Policy (CP): published document that describes all the rules and requirements which the CA abides by when setting up and providing trust services.
It notably indicates whether a Certificate applies to a particular community and/or class of applications with common security requirements. It also identifies the obligations and requirements of the various stakeholders, as well as those of all the components involved in the management of the life cycles of Certificates.
The CP is identified by an OID.

Certification Practice Statement (CPS): identifies the practices (Organization, operational procedures, technical and human resources) that the CA implements as part of the provision of its electronic Certification services to users, in accordance with the CP(s) which it has undertaken to comply with.

Certification status information service: see subsection 1.3.1

Document: static electronic document in PDF format.

Electronic identification: 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 registration file: electronic data container that contains all the data transmitted by a Subscriber during a Certificate creation request (information for the Certificate, Subject identification data...). These data are archived in a system that produces archives with evidentiary value. The CA can consult this system at any time.

Electronic seal: electronic data that are logically attached to or associated with other electronic data to guarantee the latter's origin and integrity.

Electronic signature: as per the eIDAS European Regulation, an electronic signature consists of electronic data that are logically attached to or associated with other electronic data, and which the Signatory uses to sign.
As per the French Civil Code, the signature serves to identify the person who uses it, express this person's consent, and guarantee the integrity of the act which it is associated with.

NB: the electronic signature implemented in this CP/CPS does not meet the definition of the qualified signature. As per the eIDAS European Regulation, the legal effect and admissibility of an electronic signature as legal proof cannot be refused on the sole ground that this signature is in an electronic form or that it does not meet the requirements of the qualified electronic signature.

Hash or digest: result of a calculation function performed on digital content so that even the smallest change made to that content causes the hash to change. The hash is used to identify data and verify their integrity over time.

Holder Certificate: type of Certificates issued by a subordinate CA to Subjects or Organizations. One-time-use Certificates and Organization Certificates are holder Certificates.

Key Pair: a Key Pair consists of a private key (which must be kept secret) and a public key. This combination is needed to implement a cryptography service based on asymmetrical algorithms (e.g. RSA).

Lightweight Certificate policy (LCP): certification policy defined by the [ETSI] organization.

ORG Certificate: also referred to as Organization Certificate or Electronic Seal; see subsection 1.4.2.

Organization: entity that notably represents a company, public administration, etc. or which may refer to a brand or company name for which an Organization Certificate or an electronic seal will be issued at a Subscriber's request.

OTU Certificate: also referred to as one-time-use Certificate; see subsection 1.4.1.

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

PKI component: hardware platforms (computers, HSMs, smart card readers) and software products playing specific roles within the PKI.

Registration Authority (RA): authority in charge of receiving Certificate requests from the Subscriber, verifying them, archiving them and forwarding them to the CA. The term also refers to the technical entity in charge of implementing the Registration service. Further information is provided in subsection 1.3.2.

Relying party: in the context of this CP/CPS, the relying party is the entity that uses the Certificate that it receives (here through an electronic signature, which is associated with a Document).

Registration service: see Registration Authority.

Revocation Management Service: see subsection 1.3.1

Signatory: natural person identified in one or more electronic documents and who creates an electronic signature for them.

Signing session: operation that takes place between the signing request and the return of the document(s) signed by the natural or legal person specified in the request. Several successive signatures can be carried out with the same Certificate during a signing session.

Subject: natural person identified in the Certificate as its possessor. The generation and exclusive use of the private key associated with the public key specified in the Certificate are entrusted to the Certificate Holder Mechanism.

Subordinate CA Certificate: category of Certificates issued by the Root CA to sign subordinate CAs' Certificates and revocation lists.

Subscriber: entity that signs the Subscription Contract with the OTU CA for the latter to issue

- Organization Certificates at the request of duly authorized persons within the Subscriber who are associated with by law or agreement; and
- one-time-use Certificates on behalf of Subjects as defined in this CP/CPS, whom the Subscriber will have identified beforehand, or who will have been identified, under its own responsibility, by duly authorized persons attached to the Subscriber by agreement.

The Subscriber is in direct contact with the RA and performs verifications for it, notably concerning the identity and possibly the attributes of the Subjects who use the Certificates.
With regard to OTU Certificates, the Subscriber is mandated by Subjects to request Certificates on their behalf.

Subscription Contract: contract signed between the CA and the Subscriber, and which consists of the documents which it refers to.

Technical Certification Authority (TCA): Certification Authority acting under the name of the OTU Certification Authority.

User: see Relying Party

1.7.2 Abbreviations

The acronyms used in this CP/CPS are

- **ARL:** Authority Revocation List
- **CA:** Certification Authority
- **CC:** Common Criteria
- **CISO:** Chief Information Security Officer
- **CN:** Common Name
- **CP:** Certification Policy
- **CPS:** Certification Practice Statement
- **CRL:** Certificate Revocation List
- **CSR:** Certificate Signing Request
- **DN:** Distinguished Name
- **ETSI:** *European Telecommunications Standards Institute*
- **HSM:** Hardware Security Module
- **ISP:** Information Security Policy
- **KC:** Key Ceremony
- **OID:** Object Identifier
- **OSCP:** Online Certificate Status Protocol
- **OSP**: Operational Security Policy
- **OTU CA:** Certification Authority that delivers the Certificates described in this CP/CPS

- **PKI:** Public Key Infrastructure
- **RA:** Registration Authority
- **RCA:** Root Certification Authority
- **RFC:** Request For Comment
- **RO:** Registration Operator
- **RSA:** Rivest Shamir Adelman
- **SHA:** Secure Hash Algorithm
- **TA:** Timestamping Authority
- **URL:** Uniform Resource Locator
- **UTC:** Universal Time Coordinated

2 Responsibilities with regard to the information that must be published

2.1 Entities in charge of making the information available

The OTU CA is the entity responsible for making available the information that must be published.

Indeed, to provide the information that must be published for the users of the Certificates generated by the OTU CA, the latter implements a publication function and a Certificate status information function by means of an OCSP responder and the publication of CRLs on its website.

Notably, the OTU CA is responsible for publishing this CP/CPS on its website.

2.2 Information that must be published

The information that the OTU CA publishes on its website is

- Certificate Revocation Lists (CRLs),
- this CP/CPS in French and English,
- older versions of CPs in French and English,
- the Terms of Service (TS) in force,
- the General Terms of Subscription (GTOS) in force,
- the General Terms of Sale (GTS) in force,
- the address for accessing the OTU CA's OSCP responder,
- the valid OTU CA Certificate, and
- the Certificates of the test range.

The URLs for accessing this CP/CPS, the CRL and the OCSP responder are available in the extensions of the Certificates issued by the OTU CA in accordance with section 7.1 of this document.

The Subscriber can request the Proof Management Policy (PMP) electronically (via e-mail).

The OTU CA's website is available 24 hours a day, 7 days a week. The site is monitored by teams of the Atos group. This site's address is https://www.mediacert.com
This page containing the published information has a high level of availability, with a 99.8% uptime requirement.

2.3 Publication time and frequency

The time and frequency at which the Certificate status information is published, and the availability requirements applicable to this information, are specified in subsections 4.9.7, 4.9.8 and 4.10.2 of this document.

It must be noted that the previous versions of contractual documents (GTOS) exclusively govern the periods of time covered by these versions i.e. until Subscribers are notified of their replacement. As soon as a new version is published and Subscribers have been notified of this publication, it will apply immediately, provided the changes made

- only concern editorial details, or changes pertaining to the state of the art and regulations;
- have no consequences on the clauses of the higher-level contract attached to the GTOS; and
- are necessary for monitoring the quality of trust services.

However, should the changes affect the economy of the higher-level contract associated with the GTOS, the parties will refer to the terms set out in the latter.
The OTU CA warns, within a reasonable time, the Subscribers that have one or more Organization Certificates of any modification of the TS, GTOS, GTS and of this CP/CPS (see section 9.11) so said Subscribers become aware of the changes that may or may not affect them. These documents are reviewed regularly, in accordance with the content of section 9.12. In addition, they are published on the OTU CA's website at the end of this notice period.

The OTU CA's Certificate is published after it has been generated and before any Certification.

2.4 Access restrictions applicable to the published information

All the information published on the OTU CA's website is accessible in read-only mode. Moreover, the documents uploaded to this website are authentic and certified as such by the presence of an electronic signature.

Write access to the systems used to publish Certificate status information (i.e. adding, deleting or modifying the published information) is strictly limited to the authorized functions of the OTU PKI. This write access is carried out through strong authentication on specific access control servers.

Write access to the other information is strictly limited to the authorized internal administration functions of the OTU PKI. Access control is performed by specific servers.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The names used comply with the specifications of the X.500 standard.

In every Certificate that complies with the X509 standard, the *Issuer* (Issuer CA) and *Subject* (Subject) fields are identified using an X.501 *Distinguished Name* (DN) in the form of a *PrintableString.*

3.1.2 Necessity of using explicit names

3.1.2.1 One-time-use Certificates

In the case of one-time-use Certificates, the Certificates issued in the name of the Subject as per this CP/CPS contain the forename and surname that appear on the valid proof of identity submitted by the Subject.

3.1.2.2 Organization Certificates

In the case of Organization Certificates, the Certificates issued contain

- the Subscriber's name, and
- the Organization's name, and
- the forename and surname that appear on the valid proof of identity submitted the person whom the Subscriber has authorized to represent that Organization; or
- the name of the unit in the Organization for which the Certificate is intended.

3.1.3 Anonymization or pseudonymization of holders

The notions of anonymization or pseudonymization are not used.

3.1.4 Rules for interpreting different name forms

The interpretation of information such as the *Distinguished Name* field is specified in each Certificate template, in chapter 7 of this CP/CPS.

3.1.5 Name uniqueness

The *Distinguished Name* (DN) field is unique for each Subject or Organization. The RA will reject any request from the Subscriber that does not comply with this rule (see subsection 4.2.1).
Therefore, throughout the OTU CA's life cycle, and after it has ceased to operate, a *Distinguished Name* (DN) assigned to a Subject or Organization cannot be assigned to another Subject or Organization.

The rules applied to obtain this uniqueness of DNs are

- For One-time-use Certificates, uniqueness is guaranteed by the *SERIALNUMBER* field of the DN.

- For Organization Certificates, uniqueness is guaranteed by the *SERIALNUMBER* field of the DN but also by the *Organization ID* field of the DN, which must be unique for each Organization. The second part of the rule is verified in particular by the RA.

More information about the construction of some of these fields is available in section 7.1 of this document.

3.1.6 Identification, authentication and role of registered trademarks

This information is available in paragraph 3.2.2.2 of this CP/CPS.

3.2 Initial identity validation

3.2.1 Method for proving the possession of the private key

3.2.1.1 One-time-use Certificates

For Certificates designed to be used over short periods of time (see subsection 6.3.2), the possession of the private key is verified by means of the low-level cryptographic verification of a first signature produced using the private key.

If the verification fails, then

- The document is not signed.
- The private key is destroyed (see paragraph 6.2.10.2).
- The Subscriber who made the request receives an error message indicating that this request failed.

The Certificate's Subject is not subjected to this proof of possession.

3.2.1.2 Organization Certificates

The proof of possession of the private key provided by the Certificate Holder Mechanism is guaranteed, during the generation of the request, by the signature of the message with the private key corresponding to the public key contained in the PKCS #10 message sent to the RA.

These request formats include a signature with the corresponding private key, which guarantees the integrity and proof of possession of the private key.

The authorized individual specified in the Certificate is not subjected to this proof of possession.

3.2.2 Validation of Organizations' identities

3.2.2.1 Validation of a Subscriber

The validation of a Subscriber's identity requires that the steps below be followed and that all the required information be collected. The RA keeps all the documents transferred as part of the Subscriber's subscription to the service.

3.2.2.1.1 Prior signing of a Subscription Contract

The "Subscriber" status is conditioned by the prior establishment of a contractual relationship between the Subscriber and the OTU CA. This is the Subscription Contract, through which the Subscriber subscribes to the one-time-use electronic signature service and/or the electronic seal service. The signing of this Subscription Contract notably attests to the Subscriber's acceptance of its obligations, which are described in section 9.6 of this document, and of the GTOS (documents enclosed with the Subscription Contract).

3.2.2.1.2 Designation or appointment of representatives within the Subscriber for one-time-use or Organization Certificate creation requests

A representative of the Subscriber must then be designated and declared as such to the RA so they become the RA's contact for Organization Certificate requests. This representative of the Subscriber can be

- the Subscriber's legal representative (as it appears in a company registration certificate of the Subscriber less than three months old);
- its contractual representative (as it appears, for example, in the statutes); or
- a representative authorized by the legal representative to represent the Subscriber as part of the execution of the Subscription Contract.

The Subscriber, through its legal or statutory representative, may formally appoint in writing one or more deputy Subscriber representatives who are allowed to represent it (This is done through the information sheet of the OTU CA Subscriber's Deputy Representative, which is provided by the RA.). To do so, the Subscriber must inform the RA and give the aforementioned persons the necessary powers.

3.2.2.1.3 Documents to be provided for the signature of Subscription Contract

In addition, when signing the Subscription Contract, the designated representative of the Subscriber must provide

- the information sheet of the OTU CA Subscriber's representative—which is provided by the RA— duly completed and signed by said representative. This form contains, among other things, the Subscriber's physical address and a valid e-mail address that can be used to contact its representatives. Among other things, this e-mail address will be used to send information during the creation of Organization Certificates.
- the identification policy that the Subscriber implements, in accordance with the RA's recommendations, only when subscribing to the one-time-use Certificate service. This policy must be validated by the RA and can be verified by the latter in accordance with paragraph 3.2.3.1.
- a copy of a valid official identity document containing an identity photograph. This document can be a national identity card of a country of the European Union, or a passport.
- a company registration certificate less than three (3) months old, or the current published statutes of the Organization which they belong to, including their name and capacity, and any valid documents needed to justify their powers.
- if they do not appear in the company registration certificate less than three (3) months old, or in the current published statutes of this Organization, they must be duly authorized by the Subscriber's legal representative to represent the Subscriber by means of a written authorization stating all the powers granted to them.

All these elements are also listed in a document that is given to the Subscriber along with the Subscription Contract.

3.2.2.2 Validation of an Organization

As described in subsection 1.3.4, an Organization is represented by an authorized individual— the Organization's representative. The information concerning the Organization that must be provided to the RA is

Regarding the Organization

- any document that was valid at the time of the Certificate creation request and which attests to the existence of the Organization (company registration certificate less than three (3) months old or the original or copy of any official act or register less than three (3) months old that states the name, legal form, headquarters address and identity of the associates and directors specified in sections 1° and 2 ° of Article R. 123-54 of the French Commercial Code, or their equivalents in foreign law, etc.)

Regarding the Subscriber's right to include the Organization's name in the Certificate

- any document that was valid at the time of the Certificate creation request and which proves the Subscriber's right and capacity to include the Organization's name in the Certificate

- If the Certificate is intended for the Subscriber itself i.e. the Subscriber's name is the same as that of the Organization, this document is not required.

This right of the Subscriber to include the name of the Organization in the Certificate is based on the following elements:

- if the Certificate is intended for the Subscriber, a signed request less than three (3) months old by an authorized representative of the Subscriber, and which specifies:
    - the name of the Organization to be included in the electronic Certificate; and
    - the surname and forename of the individual authorized to represent the Organization and identified in the Certificate.
- if the Certificate is not intended for the Subscriber, a dated, signed request less than three (3) months old from an authorized representative of the Organization to the Subscriber, and which specifies:
    - the name of the Organization to be included in the electronic Certificate; and
    - the surname and forename of the individual authorized to represent the Organization and identified in the Certificate.
- any document that was valid at the time of the Certificate creation request and which proves that the authorized individual belongs to the Organization;
- a copy of a valid official identity document of the authorized individual, among the ones listed below:
    - National Identity Card
    - Passport
    - Residence permit

  The RA keeps this copy.
- the postal address, an e-mail address and a telephone number enabling the RA to contact this authorized individual.

This CP/CPS does not impose any physical presence requirements for identification. However, the RA may perform additional checks by phone.

3.2.3 Validation of an individual's identity

3.2.3.1 Validation of the identity of a one-time-use Certificate Subject

The Subscriber requests the creation of a Certificate from the RA on behalf of a Subject.
This request is made electronically because it must be signed by the requisitioner using an electronic signature. It contains at least the following data about the Subject:

- their forename and surname; and
- their date and place of birth.

The Subscriber can also specify for the registration file:

- the Subject's title,

- the Subject's postal address,
- the Subject's phone number, and
- the Subject's e-mail address.

The Subscriber can complete the aforementioned information with information that is known beforehand, is specific to the future Subject and makes it possible to identify them in a predefined database.

Only the "forename and surname" information of the Subject is included in the Certificate produced by the OTU CA. However, all the aforementioned information is kept by the RA in the electronic registration file associated with the issuance of the Certificate, in accordance with section 5.4 of this document.

The retention of this data is necessary because they serve to build the registration file associated with each Certificate issuance. This registration file contains the aforementioned data, thus describing the processes and identification data of the final customer (Subject).

In addition, subsection 3.1.5 of this document defines how the uniqueness of the *Distinguished Name* is guaranteed in one-time-use Certificates.

Identification policy
When contracting with the OTU CA, the Subscriber must specify in writing the identification policy that it has implemented (see subparagraph 3.2.2.1.3) to verify the civil identity declared by the future Subject.
The identification procedures contained in this policy must be based, at least, on the verification of a valid official document containing the Subject's photograph (national identity card, passport or residence permit); or on any other valid process that makes it possible or has made it possible to verify the identity declared by a Subject prior to the issuance of the Certificate.
In particular, the elements that must be collected, verified and kept are the forenames, names, date and place of birth of the person, and the nature and date of delivery of the document.

The RA reserves the right to evaluate the reliability of the identification process put in place and not to issue Certificates if the Subscriber's identification policy is considered as insufficiently reliable. In particular, the RA will verify this policy at least once a year through sampling, in accordance with the RA's sampling procedure.

During the identification process, the verifications of the future Subject's identity will have to be based on legally valid identity documents, which, in some countries, may exist in an electronic form. Indeed, in certain countries, the identification step can be carried out using an electronic identity document or other electronic identification methods recognized as legally valid ways of providing reliable identification.

In this context, the Subscriber makes sure that the Subject has a valid electronic identity document or other electronic identification methods recognized as legally valid ways of providing reliable identification.
These identity documents in physical or electronic form serve to reinforce the identification data that the Subscriber has previously collected from the Subject.

The aforementioned identification policy is completed by a description of the process that the Subject will use to consent to perform electronic signing using the one-time-use Certificate (Consent collection policy).
This consent collection policy details, for each piece of consent to be obtained as part of the implementation of this electronic signature, the identification of the means by which the Subject will express their agreement. Indeed, the Subject, before being able to sign electronically, must

- read the terms of use of the electronic signature and their obligations as described by the Subscriber in a durable document provided in readable, explicit form;
- consent to the electronic signature as part of the transaction which they are a party of by accepting the terms and conditions pertaining to the use of one-time-use Certificates;

- accept that the RA keeps a register that enables it to process and keep the necessary identity information used to generate the one-time-use Certificate, for the duration defined by the execution of its mission and the related audits;

- confirm the validity of the information contained in the Certificate;

- as a result of the previous points, give the Subscriber an express mandate so the Subscriber can send the RA a request for a one-time-use Certificate so the Subject can sign. It must be noted that, in this context, the consent given by the Subject triggers an automated electronic signature request to the RA on behalf of the Subscriber.

The Subject's consent can be expressed and collected using one of the following methods:

- an electronic capture of the Subject's' handwritten signature,

- the sending of an OTP code via SMS to the Subject's mobile phone, or

- a recording of the Subject's voice.

The list above is not exhaustive and should only be considered as an example.

Since the identification process is described by the Subscriber, it is the latter's responsibility to

- implement it or have it implemented under its own responsibility. If persons have been appointed and authorized by the Subscriber to carry out this identification under its own responsibility, this fact must be specified by the Subscriber in the identification policy which it provides the RA with.

- transmit to the RA, in an electronic registration file, the identification data captured through the implementation of the chosen process.

Exceptions to the principle of transmission to the RA of the elements that prove Subjects' identities

The Subscriber thus sends the RA digital copies of all the elements used to verify the future Subject's identity, except in the following cases:

- The Subject belongs to the Subscriber's Organization. Indeed, it is not necessary for the Subscriber to carry out an additional identity check if the Subscriber has provided the future Subject with a reliable authentication method accepted by the RA, notably for accessing their professional electronic mailbox or logging in to the application that requires the Subject's signature.

  In this context, the Subscriber must ask the future Subject to ensure the security of their computer, professional electronic mailbox and credentials.

  The RA is required to make sure that the Subject did belong to the Subscriber's Organization at the time of the signature by carrying out sampling-based checks as mentioned earlier.

- The Subscriber keeps the elements used to verify the future Subject's identity on behalf of the RA. In this context, the Subscriber must keep these elements securely. The RA will then make the necessary declarations to the CNIL (*French Data Protection Authority*) in order to meet the obligations imposed on the Certification Authorities vis-à-vis their auditors.

  The RA must ensure that the Subscriber has actually verified the future Subject's identity by carrying out sampling-based checks as mentioned earlier.

3.2.3.2 Validation of the identity of an Organization Certificate's Subject

The information is available in paragraph 3.2.2.2 – *Regarding the Subscriber's right to include the Organization's name in the Certificate*

3.2.4 Unverified information

The Certificates issued by the OTU CA in accordance with this CP/CPS do not contain unverified information except for the e-mail address and the *Organization Unit* (OR) field corresponding to the Organization's unit name within the *Distinguished Name* (DN) of the *Subject*.

3.2.5 Validation of the requisitioner's authority

Subscriber validation is described in paragraph 3.2.2.1. When requesting the creation of a Certificate, the Subscriber authenticates itself with the RA and the Certificate Holder Mechanism. This authentication varies according to the type of Certificate requested.

3.2.5.1 One-time-use Certificates

When requesting the creation of a one-time-use Certificate and a signature from the RA (which then contacts the Certificate Holder Mechanism), the Subscriber must authenticate itself and sign the request electronically.

The Subscriber is then authenticated by means of a Certificate. This Certificate must be issued by a CA approved by the OTU CA as described in the Certification Practice Technical Document [CPTD].

3.2.5.2 Organization Certificates

When the Subscriber's representative requests an Organization Certificate from the RA, the Subscriber's representative is authenticated by the RA.

The Subscriber is then authenticated by means of a signed handwritten request. The RA verifies the authenticity of this request using the signature present on the copy of the proof of identity that it keeps, and also thanks to a set of elements related to the business relationship that exists between Worldline and the Subscriber.

3.2.6 Interoperability criteria

This CP/CPS imposes no requirements in this regard.

3.3 Identification and validation of a key renewal request

3.3.1 One-time-use Certificates

As per this CP/CPS, no key renewal function exists for this type of Certificates. Indeed, as the name implies, this type of Certificate is only used once.

3.3.1.1 Identification and validation for the common renewal of a Certificate

Not applicable

3.3.1.2 Identification and validation for the renewal of a Certificate after its revocation

Not applicable

3.3.2 Organization Certificate

For this type of Certificate, a key renewal request is treated like an initial creation request. Therefore, it is not possible to issue a new Organization Certificate without also renewing the corresponding Key Pair (see section 4.6).

3.3.2.1 Identification and validation for the common renewal of a Certificate

Not applicable

3.3.2.2 Identification and validation for the renewal of a Certificate after its revocation

Not applicable

3.4 Identification and validation of a revocation request

3.4.1 One-time-use Certificates

When a Certificate with such a short life span (see subsection 6.3.2) is used, the revocation can only occur while this Certificate is used during a signing session. This is why a Subject's Certificate can only be revoked at the request of the Certificate Holder Mechanism (see paragraph 4.9.2.1).

This request is thus sent by the Certificate Holder Mechanism to the RA, which then redirects it to the OTU CA. The latter automatically validates the request and then performs the revocation immediately.

Any request for the revocation of a one-time-use Certificate coming from the Certificate Holder Mechanism is considered as valid.

3.4.2 Organization Certificates

An Organization Certificate can be revoked by

- the individual authorized and specified in the Certificate in question, or a person explicitly authorized and designated by them. The request is then sent to the RA, which forwards it to the CA so the latter validates and executes it if the request is valid.
- the CA that issued the Certificate.

The identification is then carried out as defined in paragraph 4.9.3.2.

4 Operational requirements with regard to the life cycle of Certificates

4.1 Certificate request

4.1.1 Origin of a Certificate request

4.1.1.1 One-time-use Certificates

The creation of a one-time-use Certificate can only be requested by a Subscriber identified by the RA (see paragraph 3.2.2.1). Before making any request to the RA, the Subscriber undertakes to identify the future Subject, or have them identified under its own responsibility, and to collect the Subject's consent as described in paragraph 3.2.3.1 so this Subject can benefit from the signature service provided by the OTU CA.

4.1.1.2 Organization Certificates

The creation of an Organization Certificate can only be requested by a Subscriber identified with the RA though its representative or deputy representative, in accordance with paragraph 3.2.2.1.

4.1.2 Process and Responsibilities when establishing a Certificate request

4.1.2.1 One-time-use Certificates

All the information that must be, at the very least, included in the request is specified in paragraph 3.2.3.1 of this CP/CPS.

The request is drawn up by the Subscriber on the basis of information that it will have collected from reliable sources, and of valid supporting documents obtained from the Subject (see paragraph 4.1.1.1).

Through the Subscription Contract, the Subscriber undertakes vis-à-vis Worldline to

- inform the RA, through the provision of its Identification Policy in written form, of the procedures that it wishes to implement in order to identify future Subjects;
- implement the aforementioned methods for identifying future Subjects, which are defined in its Identification Policy, in accordance with paragraph 3.2.3.1 and apply them before making Certificate creation request on behalf of the future Subject;
- inform the future Subject of the various steps that they will have to follow to obtain a Certificate in their name so they can electronically sign the document(s) that the Subscriber will submit to them and, for this purpose, obtain the future Subject's prior agreement with the choice of the electronic signature to sign these documents, and with the obligations that this choice entails (as specified in paragraph 3.2.3.1) and notably the obligation to empower the Subscriber to request one-time-use Certificates from the RA for the benefit of the Subject;
- inform the future Subject of the processing operations performed by the RA on their personal information and, for this purpose, obtain from the Subject the necessary prior consent to the processing and storage of their data as part of the generation of the one-time-use Certificate and of proof management;
- provide all the information required for the issuance of the Certificate.

Once the request has been transmitted to and validated by the RA, the latter sends it to the CA so the one-time-use Certificate in the name of the Subject is generated.

The OTU CA cannot be held liable if the Subscriber and/or the Subject do not meet the obligations that they accepted to be able to benefit from the signature service provided by the OTU CA.

The OTU CA reserves the right to refuse the issuance of a one-time-use Certificate if it turns out that the obligations of the Subject, who is related to the Subscriber, and/or the Subscriber's obligations are not met.

4.1.2.2 Organization Certificates

All the information that must be, at the very least, included in the request is specified in paragraph 3.2.3.2 of this CP/CPS.

The request is drawn up by the Subscriber's representative through an Organization Certificate request file. This file is completed by the authorized representative of the Organization and then sent to the RA, which processes the request as defined in paragraph 4.2.1.2 of this document.

The OTU CA cannot be held liable if the Subscriber does not meet the obligations that it accepted as part of the Subscription Contract signed with the OTU CA.

The OTU CA reserves the right to refuse to issue an Organization Certificate if it turns out that the Subscriber's obligations are not met.

4.2 Certificate request processing

4.2.1 Execution of the request identification and validation processes

4.2.1.1 One-time-use Certificates

Once the RA has received the Subscriber's request, it performs the following operations:

- verification of the Subscriber's identity (see paragraph 3.2.2.1): the RA verifies the information given by the Subscriber and makes sure that it does know the Subscriber.
- verification of the request: the RA verifies that the Subscriber's request is signed electronically in its name.
- validation of the Subject's identity data: the RA validates the presence of the necessary information (see paragraph 3.2.3.1). The signature of the request, carried out by the Subscriber, certifies that the information provided is valid and can be included in the Certificate.

Once these operations have been performed, if everything is correct, the RA sends the Certificate generation request to the OTU CA and keeps a trace of the Subscriber's request in the form of a digital archive.

The OTU CA will generate a Certificate containing the Subject's identity data as defined in subsection 7.1.30 of this document.

Otherwise, the request is rejected (see paragraph 4.2.2.1).

4.2.1.2 Organization Certificates

Once the RA has received the Subscriber's representative's request, it performs the following operations:

- validation of the identification data of the Organization and the individual who represents it within the Organization: completeness, uniqueness and accuracy of the information;
- verification of the completeness of the Organization Certificate request file. The RA notably ensures that it has information that enables it to contact the future Subject of the Certificate.

Once these operations have been performed, if everything is correct, the RA sends the Certificate generation request to the OTU CA and keeps a trace of the Subscriber's representative's request in the form of a digital archive.

Otherwise, the request is rejected (see paragraph 4.2.2.2).

4.2.2 Acceptance or rejection of the request

4.2.2.1 One-time-use Certificates

Acceptance or rejection is automatic.

If the request is rejected, the RA informs the Subscriber by means of a technical notification in response to the Subscriber's request. This notification includes the reason for the rejection. A new request must be made.

4.2.2.2 Organization Certificates

Acceptance or rejection is manual.

If the request is rejected, the RA informs the point of contact identified in the request and justifies the rejection. The RA can then request the missing documents in order to complete the registration file, but cannot modify the signed data in any case whatsoever. A new request must be made.

4.2.3 Time needed to create the Certificate

4.2.3.1 One-time-use Certificates

Once the request for the creation of a one-time-use Certificate has been validated, the Certificate is generated immediately.

4.2.3.2 Organization Certificates

Once the request for the creation of an Organization Certificate has been validated, the Certificate is generated as soon as possible.
A specific technical document summarizing the generation of the Certificate and listing the technical participants is created and kept as an execution log.

4.3 Certificate issuance

4.3.1 CA's actions regarding the issuance of the Certificate

After authenticating the origin and verifying the integrity of the request coming from the RA, the OTU CA initiates the Certificate generation process. The conditions under which keys and Certificates are generated as well as the security measures that must be complied with are specified in chapters 5 and 6 of this CP/CPS. Once the Certificate is generated, the OTU CA sends it to the Certificate Holder Mechanism through the RA. The Certificate Holder Mechanism guarantees the security of Key Pairs in accordance with the content of paragraph 6.1.1.4.

4.3.1.1 One-time-use Certificates

In the case of one-time-use Certificates, the Certificate produced is accessible to the Subject in the signature of the document(s) for which the Certificate has been issued.

4.3.1.2 Organization Certificates

In the case of Organization Certificates, the Certificate produced is also sent by e-mail to the Subscriber's representative.

4.3.2 Certificate delivery notification sent by the CA

The OTU CA sends the Certificate produced to the Certificate Holder Mechanism through the RA in response to the processing of the Certificate creation request. This operation is logged in the RA's logs. This transmission has the same value as a notification.

4.3.2.1 One-time-use Certificates

Not applicable

4.3.2.2 Organization Certificates

When an Organization Certificate is issued, it is also sent to the Subscriber's representative so they validate the information that it contains before it can be used (see paragraph 4.4.1.2). This, by express convention, is equivalent to a notification.

4.4 Certificate acceptance

4.4.1 Certificate acceptance process

4.4.1.1 One-time-use Certificates

The Subject's identification data and the result of their processing to form the Certificate's data are explicitly validated by the Subject before the Certificate is issued. This validation is then kept in the corresponding registration file.

Indeed, given the atomic nature—computer-wise— of the signing operation in the context of use of a one-time-use Certificate, the data contained in the Certificate are validated before the Certificate is issued.

In addition to this validation, automatic checks are carried out by the Certificate Holder Mechanism to detect possible nonconformities before the Certificate is issued.

4.4.1.2 Organization Certificates

The Organization Certificate produced by the OTU CA is sent to the Subscriber so it is validated before use, in accordance with the content of subsection 4.3.1 of this document.

This CP/CPS requires the explicit acceptance of the information specified in the Certificate either from the legal or statutory representative of the Subscriber who made the request, or from of the authorized individual identified in the Certificate. This explicit acceptance, which is expressed via an e-mail sent to the address provided during the constitution of the subscription file, is considered as sufficient. Indeed, the e-mail address of the issuer that was enrolled during the constitution of the subscription file is deemed as authenticating the origin of the acceptance of the Certificate.

The Certificate Holder Mechanism cannot use an Organization Certificate in any way whatsoever without this acceptance phase.

4.4.2 Certificate publication

No service publishes the Certificates issued by the OTU CA. Only the OTU CA's Certificate is published (see section 2.2).

4.4.3 Notification sent by the CA to inform other entities of the delivery of the Certificate

Not applicable

4.5 Use of the Key Pair and the Certificate

4.5.1 Use of the private key and the Certificate by the Certificate Holder Mechanism

The use of the private key and the associated Certificate by the Certificate Holder Mechanism is strictly limited to the signing service described in paragraph 1.5.1.1 of this document. Otherwise, the OTU CA may not be held liable.

Moreover, the authorized use of the Key Pair and the associated Certificate is specified in the Certificate by means of the key usage extensions.

4.5.2 Use of the public key and the Certificate by relying parties

As explained in subsection 4.5.1 above, Subscribers, and the persons who are associated with them and request Certificates, must comply with the use stipulated in the Certificates that the OTU CA produces at their request. They must thus refuse any other use of the Certificate. Otherwise, the Subscribers and the related persons who requested a Certificate may be held liable.

4.6 Certificate renewal

This CP/CPS prohibits Certificate renewal (new Certificate without a change of key).

4.6.1 Possible reasons for Certificate renewal

Not applicable

4.6.2 Origin of a renewal request

Not applicable

4.6.3 Processing of a renewal request

Not applicable

4.6.4 Notification of creation of the new Certificate

Not applicable

4.6.5 Acceptance of the new Certificate

Not applicable

4.6.6 Publication of the new Certificate

Not applicable

4.6.7 Notification sent by the CA to inform other entities of the delivery of the new Certificate

Not applicable

4.7 Delivery of a new Certificate following a change of Key Pair

The issuance of a new Certificate related to the generation of a new Key Pair is treated like an initial Certificate creation request.

The use of an existing Key Pair associated with a former CSR is prohibited.

4.7.1 Possible reasons for a change of Key Pair

Not applicable

4.7.2 Origin of a request for a new Certificate

Not applicable

4.7.3 Processing of a request for a new Certificate

Not applicable

4.7.4 Acceptance of the new Certificate

Not applicable

4.7.5 Publication of the new Certificate

Not applicable

4.7.6 Notification sent by the CA to inform other entities of the delivery of the new Certificate

Not applicable

4.8 Certificate modification

Certificate modification is prohibited by this CP/CPS.
However, the modification of an Organization Certificate amounts to revoking the Certificate in question, and then requesting a new one in accordance with the procedure described in paragraph 4.1.1.2.

4.8.1 Possible reasons for Certificate modification

Not applicable

4.8.2 Origin of a Certificate modification request

Not applicable

4.8.3 Processing of a Certificate modification request

Not applicable

4.8.4 Acceptance of the modified Certificate

Not applicable

4.8.5 Publication of the modified Certificate

Not applicable

4.8.6 Notification sent by the CA to inform other entities of the delivery of the modified Certificate

Not applicable

4.9 Revocation and suspension of Certificates

Certificate suspension is prohibited by this CP/CPS.

4.9.1 Possible reasons for a revocation

4.9.1.1 One-time-use Certificates

The following circumstances can result in the revocation of a Subject's one-time-use Certificate:

- The Subject's information contained in the Certificate that has been issued in their name does not conform to the Subject's identity as received from the Subscriber.
- The information concerning the use of the Certificate appearing in the Certificate does not conform to that one provided for by the framework defined in paragraph 1.5.1.1.
- An intentional or unintentional error has been detected in the Subject registration request.
- An incident occurred when the Certificate Holder Mechanism used the Subject's Certificate for a signing operation as part of the normal use defined in section 1.5.
- The private or public keys do not match, or the Certificate Holder Mechanism is unable to use them as part of the normal use defined in section 1.5.

When one of the aforementioned events occurs, and the CA is aware of it, the Certificate concerned must be revoked immediately. However, given the use of the one-time-use Certificates produced under this CP/CPS and the short life span of these Certificates, it is important to note that revocation here is primarily an instrument used to provide a CRL for the technical components that must have one.

For this type of Certificates, the reason for the revocation is not published.

4.9.1.2 Organization Certificates

The following circumstances can result in the revocation of the Organization Certificate:

- The Organization's information that appears in the Certificate that was issued in its name does not conform to the Organization's identity or the use specified in the Certificate.
- An intentional or unintentional error has been detected in the Organization registration request.
- The verification of the holder's private key is suspected to have failed, or the holder's private key is
    - suspected of being compromised,
    - compromised,
    - lost,
    - stolen,
    - destroyed,
    - tampered with.
- The authorized representative (see subsection 3.4.2) requests the revocation of the Certificate.
- The CA's, Organization's or Subscriber's activity comes to an end.
- The contractual relationship between the Subscriber and the CA ends.
- Changes occur in the technical or legal regulations, or in the recommendations applicable to the CA or the Organization, thus requiring that the Certificate no longer be used.

When one of the aforementioned events occurs, and the CA is aware of it, the Certificate concerned must be revoked immediately.

In addition, the CA is allowed to revoke a Certificate as of right under the following circumstances:

- non-compliance with this CP/CPS;
- A Subject or the Subscriber fails to meet any of the obligations resulting from the Subscription Contract or from any other document contained in the subscription file (such as this CP/CPS and section 9.6 thereof), notably if the Certificate is used under conditions other than those provided for by this document (see section 1.5).

For this type of Certificate, the reason for the revocation is published. This, in particular, makes it possible to identify the type of Certificate in the CRL.

4.9.1.3 Certificate of a PKI component

The following events can result in the revocation of a Certificate of an OTU PKI component (including the OTU CA's Certificate):

- suspicion of compromise, compromise, loss or theft of the private key;
- The content has been altered following a change (nonconformity correction, change made to the Certificate template, etc.).
- cessation of activity, or
- regulatory changes in the algorithms used.

When any of the aforementioned circumstances occur and Worldline becomes aware of it, Worldline decides to revoke the Certificate in question of the OTU PKI component concerned.

4.9.2 Origin of a revocation request

4.9.2.1 One-time-use Certificates

Only the Certificate Holder Mechanism is authorized to request the revocation of this type of Certificate after one of the circumstances specified in paragraph 4.9.1.1 of this document occurs.

4.9.2.2 Organization Certificates

The persons and entities authorized to request the revocation of this type of Certificate, after one of the circumstances specified in paragraph 4.9.1.2 of this document occurs, are

- the Subscriber's representative or one of the Subscriber's deputy representatives who has the identification and authentication data that enable them to access this function; and
- the OTU CA.

4.9.2.3 Certificate of a PKI component

The revocation of the OTU CA's Certificate or of the other Certificates of OTU PKI components may only be decided by Worldline or legal authorities following a court ruling.

4.9.3 Processing of a revocation request

4.9.3.1 One-time-use Certificates

This CP/CPS imposes no requirements with regard to the identification of the revocation request. Indeed, only the Certificate Holder Mechanism as described in subsection 1.3.3 is allowed to request a revocation if one of the possible causes for revocation is detected (see paragraph 4.9.1.1).

Therefore, the request is automatically authorized. The OTU CA then performs the revocation. The operation is instantaneous and is logged in the event logs (see subsection 5.4.1).

Once revoked, the Certificate cannot be restored. The Subject concerned is informed of the change of status through the publication of the revoked Certificate in one of the CRLs published at the address defined in section 2.2 of this document.

4.9.3.2 Organization Certificates

For this type of Certificate, revocation requests are not authorized automatically. Indeed, the request made by the authorized person or entity (see paragraph 4.9.1.2) must be validated by an authorized Worldline employee (called "Pilot"). For this purpose, the person or entity authorized to make the request calls a number given during the creation of the Certificate to be revoked. This number is available 24 hours a day, 7 days a week. The information that must be given to the Pilot for the revocation to be authorized:

- identification elements: Organization's name and identity of the authorized representative; and
- an authentication element i.e. a secret code provided during the creation of the Certificate.

Once these elements are validated by the system, the revocation request is authorized. The operation is carried out in several stages by the Pilot. Some steps also require the intervention of the requisitioner who must give by phone the information that the Pilot must enter or verify so the requisitioner keeps control over the operation. The operation is logged in the event logs (see subsection 5.4.1).

Once revoked, the Certificate cannot be restored. The Subject concerned is informed of the change of status through a notification sent by the RA and the publication of the revoked Certificate in one of the CRLs published at the address defined in section 2.2 of this document.

A request for the revocation such a Certificate is tracked and logged so the revocation deadline defined by the OTU CA can be complied with (see paragraph 4.9.5.2)

4.9.3.3 Certificate of a PKI component

Because of its origin, the revocation request is automatically validated for this type of Certificate. When revoking one of the Certificates of an OTU PKI component, the processing procedure is internal and depends on the reason for the request and the nature of the Certificate to revoke.

4.9.4 Revocation request deadline

4.9.4.1 One-time-use Certificates

Given the atomic nature—computer-wise— of the signing operation in the context of the use of a one-time-use Certificate, the request made by the requisitioner (see paragraph 4.9.2.1) is immediate when one of the causes listed in paragraph is encountered.

4.9.4.2 Organization Certificates

As soon as the authorized representative is aware of one of the possible reasons for revocation defined in paragraph 4.9.1.2 of this document, they must make a revocation request immediately.

4.9.4.3 Certificate of a PKI component

As soon as the authorized representative is aware of one of the possible reasons for revocation defined in paragraph 4.9.1.3 of this document, they must make a revocation request immediately.

4.9.5 Time needed by the CA to process a revocation request

The maximum time between the receipt of the revocation request and the moment it is taken into account is twenty-four (24) hours, the revocation management function being available 24 hours a day, 7 days a week.

4.9.5.1 One-time-use Certificates

A request for the revocation of a one-time-use Certificate is processed immediately after the OTU CA has received it. The revocation is effective when the Certificate in question is added to the generated CRL.

The operation is performed immediately and automatically after the request has been received and validated.

The maximum unavailability time allowed for the platform is eight (8) hours a month.

4.9.5.2 Organization Certificates

A request for the revocation of an Organization Certificate is processed immediately after the OTU CA has received it. The revocation is effective when the Certificate in question is added to the generated CRL.

Since a request for the revocation of an Organization Certificate is defined by its tracking number and its revocation date, it can easily be tracked and traced. This makes it possible to check whether the revocation deadline has been complied with or not.

The maximum unavailability time allowed for the platform is eight (8) hours a month.

4.9.5.3 Certificate of a PKI component

Any request for the revocation of a Certificate of a PKI component is processed immediately after the OTU CA has received it. The revocation is effective when the Certificate in question is added to the generated ARL/CRL.

Since a request for the revocation of a Certificate of a PKI component is defined by its tracking number and its revocation date, it can easily be tracked and traced. This makes it possible to check whether the revocation deadline has been complied with or not.

4.9.6 Requirements with regard to the verification of the revocation by Certificate users

4.9.6.1 One-time-use Certificates

In the context of the use of a one-time-use Certificate provided by the OTU CA, given the atomic nature—computer-wise—of the signing operation, this CP/CPS does not impose any requirement regarding the obligation to verify the revocation of the Certificate.

4.9.6.2 Organization Certificates

When using an Organization Certificate provided by the OTU CA, the user must check the status of the Certificate that they intend to rely on before using it. For this purpose, they can either consult the published CRLs as defined in section 2.2 of this document, or make a request to the OCSP responder at the address defined in the aforementioned section.

In addition to the status, the user must check the validity of the Certificate in question and of the corresponding Certification Chain.

4.9.7 CRL creation frequency

CRLs are created every twenty-four (24) hours. However, a new CRL can be published at any time e.g. following a revocation.

4.9.8 CRL publication deadline

A CRL is published sixty (60) minutes after its generation at the latest.

4.9.9 Availability of a system for verifying the revocation and statuses of Certificates online

An OCSP responder is available online and is accessible as described in section 2.2, thus enabling users to check the revocation and statuses of Certificates online (see section 4.10).

The revocation information provided is consistent between the various revocation information services (CRL and OCSP responder).

4.9.10 Requirements with regard to the online verification of Certificate revocation by users

The requirements regarding the online verification Certificate revocation by users comply with the content of subsection 4.9.6 of this CP/CPS.

4.9.11 Other ways of obtaining information about revoked Certificates

Not applicable

4.9.12 Specific requirements if the private key is compromised

The entities allowed to request the revocation of a Certificate must do so as early as possible after being informed that the private key has been compromised (see subsection 4.9.4).

Concerning the OTU CA's Certificate, its revocation after the private key has been compromised is clearly specified in a statement published on the OTU CA's website.

4.9.13 Possible reasons for Certificate suspension

This CP/CPS prohibits Certificate suspension.

4.9.14 Origin of a suspension request

Not applicable

4.9.15 Processing of a suspension request

Not applicable

4.9.16 Minimum and maximum durations of Certificate suspension

Not applicable

4.10 Certificate status information function

4.10.1 Operational characteristics

The OTU CA provides users with two mechanisms for the public consultation of Certificate statuses: CRLs and the OCSP responder.

CRLs are published on the Internet in v2 format. They are accessible via HTTP (s) at

- the address specified in section 2.2 of this CP/CPS;
- the address specified in the Certificate issued by the OTU CA as specified in section 7.1 of this CP/CPS.

A CRL contains the list of the Certificates issued by the OTU CA which, at the same time, have been revoked and have not expired yet (the expiry date and time of the Certificate have not been reached.). Indeed, a Certificate that has been revoked or has expired is no longer contained in the CRL. It notably contains the date of its publication as well as the date of the next publication.
CRLs are also signed by the OTU CA, which ensures their origin and integrity.
The link to the OCSP responder is specified on the Internet. It can be accessed via HTTP (s) at

- the address specified in section 2.2 of this CP/CPS;
- the address specified in the Certificate issued by the OTU CA as specified in section 7.1 of this CP/CPS.

The OTU CA guarantees the origin and the integrity of the responses provided by the OCSP responder which it provides users with.

4.10.2 Availability of the function

The Certificate status information function is available 24 hours a day, 7 days a week. The maximum unavailability time allowed for the platform is eight (8) hours a month.

4.10.3 Optional mechanisms

Not applicable

4.11 End of the relationship between the Subscriber and the CA

The end of the relationship between the Subscriber and the OTU CA is materialized by the cancellation or non-renewal of the Subscription Contract or of the service contracts that are expressly associated with it.

The RA no longer recognizes the requests transmitted and signed by the Subscriber, its representative or the latter's deputies.

The OTU CA then asks the Subscriber to make one or more requests (depending on the number of Certificates concerned) for the immediate revocation of its Organization Certificate(s).

4.12 Key escrow and recovery

This CP/CPS prohibits the escrow of the OTU CA's private keys and holder Certificates.

4.12.1 Policy and practices with regard to the recovery of the keys held in escrow

Not applicable

4.12.2 Policy and practices with regard to recovery through session key encapsulation

Not applicable

5 Non-technical security measures

The OTU PKI complies with an information security policy and has an OSP.

The latter, which notably defines the framework for the security rules applicable to the PKI's systems, takes into account the state of the art in this area and is reviewed regularly. In accordance with the Risk Analysis carried out by the OTU PKI's security officer. It is validated by the Security Committee following its review, which takes place every twenty-four (24) months at most.

5.1 Physical security measures

Physical security measures are taken by the OTU PKI to ensure that

- the resources, information systems and data used as part of the operational implementation of the OTU PKI are installed on secure premises, the access to which is controlled and reserved strictly for authorized staff.
- the access control system guarantees the traceability of the access to the premises on which the OTU PKI's resources and information are stored.
- the implementation of these checks makes it possible to comply with the separation of trusted roles provided for by this CP/CPS.

Below are some physical security measures implemented according to different categories. Clarifications are provided in the CPTD.

5.1.1 Geographical location and construction of sites

The OTU PKI is installed on Worldline's IT production sites in Vendôme and Brussels. These sites are designed to host computer and telecommunications systems. They comply with the construction requirements (regulations and standards) in force. The administrative and operational teams perform the administration and operation tasks on the Blois and Seclin sites.

5.1.2 Physical access

The sites and premises that host the OTU PKI guarantee the security of Certification resources.

On the IT production sites concerned, access to the site and computer rooms is controlled using group definitions, and access rights by zone and by time slot for these groups.
These sites operate 24 hours a day, 7 days a week.

On-site staff have PIN-code cards for accessing the areas that they have been authorized to access. Indeed, having an access card is mandatory in order to access the premises. Some more sensitive areas are subjected to additional measures such as anti-passback and/or the need for two (2) persons to be present for the premises to be opened.

The OTU PKI's servers, with their built-in HSM cards, are installed in high-security areas that notably require the mandatory authentication of two (2) authorized persons (dual control). The Vendôme and Brussels sites use an authentication system that involves cards and biometric data. The protection of these areas is reinforced by other physical security measures such as the presence of infrared barriers, presence detectors, an additional autonomous video surveillance system, and more.

Building access control is managed by local administrators on a dedicated server. The latter also stores the logs of access to the various readers as well as access control service messages.

Measures are taken to prevent the equipment, information, media and software pertaining to the OTU PKI's services from being taken out of the site without authorization.

5.1.3 Power supply and air conditioning

Measures taken to deal with power outages and simplify maintenance operations. Likewise, measures are taken to remedy failures of the air conditioning system. All these measures ensure the continuity of the services provided by the OTU PKI.

5.1.4 Vulnerability to water damage

Monitoring resources (sensors, monitoring...) are set up to prevent water damage, thus ensuring the continuity of the services provided by the OTU PKI.

5.1.5 Fire prevention and protection

Fire prevention and protection measures (detectors, fire doors...) are taken to ensure the continuity of the services provided by the OTU PKI.

5.1.6 Media preservation

As part of the OTU PKI's activities, a Risk Analysis is carried out in its scope (see subsection 9.17.2). This Risk Analysis makes it possible to identify the assets and their needs in term of security. Various media (paper-based documents, hard drives...) that are part of these assets are then kept in accordance with the defined security needs. The information on the measures put in place is detailed in the CPTD.

5.1.7 Media destruction

All the paper-based documents that contain confidential data (PIN codes, passwords, etc.) and have become useless or obsolete are destroyed using a shredder.

Physical media (disks, HSMs, etc.) undergo special temporary storage before they are ground in the presence of a bailiff. A formal report is drawn up following this destruction.

5.1.8 Off-site backups

As part of this CP/CPS, the OTU PKI performs off-site backups in accordance with the defined procedures (see [PESC]document]).

5.2 Procedural security measures

5.2.1 Trusted roles

The OTU PKI explicitly defines the trusted roles required to ensure its own operation and security.
The functions operated in all of the OTU PKI's components are distributed to various types of roles to ensure knowledge separation for sensitive tasks or roles. The trusted roles involved in the OTU PKI's Organization are

- HSM Administrator: person in charge of installing and configuring the OTU PKI's HSMs.

- System administrator: person in charge of installing, configuring and maintaining the OTU PKI's trust systems for service management. In particular, they are in charge of the daily operation of the OTU PKI's trust systems. They are allowed to perform backups of these systems.

- System Auditor: person authorized to consult the archives and all the audit data of the PKI's trust systems.

- Master of Ceremony: person in charge of managing the operations of entry, exit or destruction of keys (key ceremonies), for which they are the only point of entry.

- Security Officer: person in charge of administering the implementation of security practices and enforcing the technical constraints defined in the Risk Analysis.

- Registration Operator: person involved in the Certificate creation process.

- Secret holder: person in charge of ensuring the confidentiality, integrity and availability of secrets. They hold the secrets and physical keys to their safes. They belong to team, all of whose members have the same rights over access to the safes.

- Application Manager: person in charge of monitoring the service and its performance. They coordinate and/or perform the corrective and evolutionary maintenance of the application.

- Head of the CA: person in charge of implementing this CP/CPS as well as verifying its application. They are notably in charge of revoking a Certificate issued by the OTU CA. A member of the Security Committee, they are also in charge of approving this document, the CPTD, the Risk Analysis and the OTU PKI's OSP.

- Deputy head of the CA: person in charge of implementing this CP/CPS as well as verifying its application. They are notably in charge of revoking a Certificate issued by the OTU CA. A member of the Security Committee, they are also in charge of approving this document, the CPTD, the Risk Analysis and the OTU PKI's OSP.

- Center Manager: person in charge of implementing the procedures pertaining to the computer center that hosts the OTU PKI's systems. They are notably in charge of intervening to allow access to the OTU PKI's resources.

- Security manager: person in charge of defining, in liaison with the OTU CA, the security rules and procedures pertaining to the OTU PKI.

When a new member is enrolled in a trusted role within the OTU PKI, a document acknowledging this appointment must be signed by the person concerned. This document refers to the CPTD so that the future member of the trusted staff is aware of the description of their role and responsibilities. It specifies in particular:

- the signatory's obligations and the proper understanding thereof;

- If the CPTD is modified, the signatory will be informed.

Likewise, when a trusted role ends within the OTU PKI, a document acknowledging this cessation must be signed by the person concerned.

A verification is performed at least once a year to make sure persons all the aforementioned trusted roles are filled.

5.2.2 Number of persons required per task

According to the type of operation done, the number and roles of the persons that must be present, as participants or witnesses, may differ. Indeed, for security reasons, some sensitive tasks, such as the generation of the OTU CA's initial Certificate, require more than one person with a trusted role within the OTU PKI.

Certain trusted roles are assigned to several persons so the OTU PKI can ensure the continuity of its services without degrading the security of the services provided.

5.2.3 Identification and authentication for each role

Each entity that operates a component of the OTU PKI verifies, for each of its components, the identity and authorizations of any staff member, and possibly of the external persons who works on sensitive tasks. These checks comply with the Operational Security Policy [OSP] applied by the OTU PKI.

A written notification is produced to document every time a trusted role is assigned to a member of the OTU PKI staff.

5.2.4 Roles that require remit separation

As per this document, trusted roles can be assigned to several natural persons.
In addition, certain roles can be assigned to the same person. These roles are defined in the matrix below:

	HSM Administrator	System Administrator	System Auditor	Master of Ceremony	Security Officer	Registration Operator	Secret Holder	Application Manager	CA Manager	Deputy CA Manager	Center Manager	Security Manager
HSM Administrator		✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗
System Administrator	✗		✗	✓	✓	✗	✓	✓	✓	✓	✓	✗
System Auditor	✗	✗		✗	✗	✗	✗	✗	✗	✗	✗	✗
Master of Ceremony	✓	✓	✗		✓	✗	✓	✓	✓	✓	✓	✗
Security Officer	✓	✓	✗	✓		✗	✓	✓	✓	✓	✓	✗
Registration Operator	✓	✗	✗	✗	✗		✗	✓	✓	✓	✓	✗
Secret Holder	✓	✓	✗	✓	✓	✗		✓	✓	✓	✓	✗
Application Manager	✓	✓	✗	✓	✓	✓	✓		✓	✓	✓	✗
CA Manager	✓	✓	✗	✓	✓	✓	✓	✓		✓	✓	✗
Deputy CA Manager	✓	✓	✗	✓	✓	✓	✓	✓	✓		✓	✗
Center Manager	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓		✗
Security Manager	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	

5.3 Security measures with regard to the staff

5.3.1 Required qualifications, skills and authorizations

The staff who have trusted roles within the OTU PKI are informed of their relative responsibilities (commitment document, CPTD) as well as the procedures related to system security and staff control, which they must comply with..

The management staff are trained and aware of security and risk management so they can fully fulfill their responsibilities vis-à-vis the OTU PKI.

The OTU PKI ensures the qualification and competence of the members of its staff who have trusted roles.

5.3.2 Criminal record verification procedure

Procedures for verifying criminal records are implemented for the persons who are to have trusted roles within the OTU PKI. In particular, these persons must not have been the subject of a legal sentence that could jeopardize their participation in the OTU PKI's activities, or be in a situation in which their remit would cause a conflict of interest. For this purpose, the persons concerned must submit a copy of bulletin n °3 of their criminal record to Worldline's Human Resources department when signing the document (see subsection 5.2.1) by which they accept their role, obligations and responsibilities as part of their participation in these activities.

The applicant's application file is subjected to the validation of the Human Resources department and that of the head of the OTU CA.

Criminal records are verified every three (3) years. Consequently, a recurring yearly verification of criminal records is put in place.

The staff in charge of operating the Certification services are not responsible for the commercial aspects of these services and are free from any conflict of interest that might influence the way they perform the operations which they are in charge of and might undermine trust (see subsection 9.17.1). In this regard, they undertake to confirm in writing, upon their acceptance of the trusted role within the OTU PKI, the absence of any conflict of interest related to the exercise of this new activity.

5.3.3 Basic training requirements

The staff are trained in the software, hardware and working procedures of the OTU PKI. They understand and know what the operations which they are responsible for involve.

5.3.4 Continuous training requirements and frequency

The staff receives the necessary training before any change is made to systems, procedures, the organization or other things according to the nature of these changes. In particular, they are trained in the issues related to the security of information systems and are aware of incident handling.

5.3.5 Frequency and sequence of cycling through different assignments

Not applicable

5.3.6 Sanctions in the event of unauthorized actions

Worldline's by-laws indicate that appropriate administrative disciplinary sanctions are applicable in the event of a fault (failure to comply with this CP/CPS, etc.). The staff are reminded of this particular fact in the commitment to responsibilities that they accept when accepting their roles within the OTU PKI.

In the event of a fault (non-compliance with this CP/CPS...), the entities external to Worldline that participate in the OTU PKI's activities are subjected to sanctions defined during the contracting phase.

5.3.7 Requirements with regard to external providers' staff

The staff of the potential external contractors operating on the premises and/or components of the OTU PKI must meet the requirements set out in paragraphs 5.3.1 to 5.3.4 of this document.

5.3.8 Documents given to the staff

Each person has at least the documents pertaining to the operational procedures and the specific tools that they implement, as well as the general policies and practices of the component which they work in.

5.4 Procedures for constituting audit data

The events that occur throughout the OTU PKI's life are logged to files automatically generated by software, the output of which is completed by manual data entry if need be. These files aim to ensure the traceability and accountability of operations (authors, timestamps, etc.).

The logging process is executed on the fly for automatic systems, and for manual interventions as of the initialization of the operation at the earliest.

No manual operation can be triggered without the initialization of a traceability ticket.

Event logs explicitly include the identifier of the software or human that executes the operation.

They can be put at the disposal of the judicial system as part of a legal request by petitioners.

5.4.1 Types of events logged

The events logged in the OTU PKI's event logs are:

- startups and stops of IT systems and applications;
- startups and stops of the logging function settings;
- modifications of the settings of the logging function;
- generation of keys for the various components;
- modifications (change, correction or upgrade) of the various components;
- receipt of Certificate creation or revocation requests;
- processing (validation or rejection) of Certificate creation or revocation requests;
- Certificate generation and revocation operations;
- transmission of one-time-use Certificates and Organization Certificates to the Certificate Holder Mechanism;
- generation and publication of CRLs;
- modifications (change, correction or evolution) of this CP/CPS, the CPTD, the Risk Analysis and the OSP.

In addition, security-related events are also logged in the OTU PKI's event logs. Here is a non-exhaustive list of these events:

- physical access to the premises that host the OTU PKI;
- changes made to the technical platform (maintenance, software upgrade);

- changes in the staff involved in the OTU PKI;
- purging or destruction of expired Certificates;
- pilots' monitoring and management actions;
- creation / modification / deletion of user accounts and the corresponding authentication data;
- logins and logouts of users who have trusted roles within the OTU PKI (including the corresponding failed attempts);
- events related to signature keys and CA Certificates (generation during a key ceremony, backup, recovery, revocation, renewal, destruction, etc.).

Logged events contain all the information that makes it possible to identify and analyze them. This information consists of

- types of events,
- date and time of the event,
- persons involved – software component or human intervention,
- context: (scheduled operation with a requisitioner, operational intervention following a malfunction, etc.),
- result – success or failure,
- possible relation to other events.

The person, organization or system that executed an action is accountable for it. The name or identifier of this operator is specified explicitly in a field of the event log as defined above.

5.4.2 Event log processing frequency

Event logs are collected on the fly and are inspected in real time.

5.4.3 Event log retention period

The electronic event logs are saved every day for a period of three (3) months and are archived periodically (see subsection 5.5.6) for a duration defined in subsection 5.5.2 of this document.

The handwritten event logs are stored and kept as defined in subsection 5.5.2 of this document.

5.4.4 Event log protection

The electronic event logs are collected and outsourced to two types of environments that are administered differently. Therefore, only the personnel authorized by the OTU PKI as defined in the CPTD can access these elements, which cannot be modified without authorization.

The handwritten event logs are protected by secure physical systems (safe or strong cabinet).

5.4.5 Event log backup procedure

The OTU PKI's event log backup procedure is internal and is specified in the CPTD.

5.4.6 Event log collection system

The OTU PKI's event log collection system is internal and is specified in the CPTD..

5.4.7 Transmission of an event logging notification to the person responsible for it

The person responsible for an event does not systematically receive a notification that informs them of the fact that this event has been logged.

5.4.8 Evaluation of vulnerabilities

Event logs are analyzed using a tool specified in the CPTD that also produces a report accessible to the controller entity for analysis and monitoring, at regular intervals or following an alert launched by the same tool.

5.5 Data archiving

The data that must be archived are archived in accordance with the practices set out below.

5.5.1 Type of data to archive

The archiving is carried out by the OTU PKI to ensure the traceability and accountability of operations. The data that must be archived vary according to the entities.

5.5.1.1 CA and RA

For the CA and RA of the OTU PKI, the archived data are

- registration information,
- Certificate generation requests,
- Certificate revocation requests,
- Certificates and CRLs,

5.5.1.2 Technical platform

For the OTU PKI's technical platform, the archived data are

- the technical documents that describe IT configurations and equipment,
- software operation settings,
- operation procedure documents,
- the daily operation register; and
- event logs.

5.5.1.3 Documentation

For the OTU PKI's documentation, the archived data are:

- key ceremony manuals,
- versions and revisions of this CP/CPS,
- versions and revisions of the CPTD,
- versions and revisions of the Risk Analysis; and
- versions and revisions of the OSP.

5.5.2 Archive retention period

5.5.2.1 CA and RA

CRL archives are kept until the end of the life of the CA.

5.5.2.1.1 One-time-use Certificates

The retention period of the registration file archives is eight (8) years from the moment when the validation of the file by the RA and the finalization of the processing of the file by the Subscriber were confirmed.

However, the retention period for registration files may be modified at the request of the Subscriber, who may request from Worldline an extension beyond these eight (8) years, by express agreement under conditions specific to the Subscription Contract. This extension must be justified by regulatory or legal constraints. Moreover, it entails for the Subscriber the obligation to inform the persons concerned by the processing of the personal data contained in the registration files.

Certificate creation and revocation requests are kept for eight (8) years from the moment of their receipt.

5.5.2.1.2 Organization Certificate

The retention period of the registration file archives is ten (10) years from the moment when the validation of the file by the RA and the end of processing of the file by the Subscriber were confirmed.

However, the retention period for registration files may be modified at the request of the Subscriber, who may request from Worldline an extension beyond these ten (10) years, by express agreement under conditions specific to the Subscription Contract. This extension must be justified by regulatory or legal constraints. Moreover, it entails for the Subscriber the obligation to inform the persons concerned by the processing of the personal data contained in the registration files.

Certificate creation and revocation requests are kept for ten (10) years from the moment of their receipt.

5.5.2.2 Technical platform

Event logs are kept for ten (10) years from their creation.

5.5.2.3 Documentation

Documentary archives are kept for ten (10) years after the last issuance of a Certificate by the OTU CA before the cessation of its activity.

5.5.3 Archive protection

During the retention of archives on the OTU PKI's secure premises, their integrity is protected, and only authorized persons can access them. Indeed, to ensure the confidentiality of information, the request for accessing an archive can only be made by the head of the CA, a deputy head of the CA or the OTU PKI's security officer,

Procedures are put in place to prevent the obsolescence and deterioration of the archives. In particular, they are stored on premises subjected to protective measures against natural hazards.

5.5.4 Archive backup procedure

Archives benefit from the same level of protection as backups. Archive backup procedures are internal and are specified in the CPTD.

5.5.5 Data timestamping requirements

Timestamping requirements are specified in section 6.8 of this document.

5.5.6 Archive collection system

Archives are produced once a month. The method used to collect archives is internal and is specified in the CPTD.

5.5.7 Archive recovery and verification procedure

Archives can be recovered in less than two (2) working days from the registration of the request. The access to archives is subjected to restrictions (see subsection 5.5.3).

5.6 Change of the CA's key

The OTU CA may not issue Certificates whose validity dates (start dates or end dates) exceed the expiry date of the Certificate with which it would issue the Certificate.

If one of the OTU CA's Certificates expires, it will be renewed during the year preceding its expiry date to ensure the continuity of the operations of the entities that use the Certificate in question.

As soon as a new Key Pair of the OTU CA is generated, only the new private key is used to sign Certificates.

The previous Certificate can no longer be used within the framework defined for it i.e. to sign Certificates and CRLs (see chapter 0). However, it remains accessible to validate the Certificates signed with the corresponding private key until the last of these Certificates has expired.

The CA may not reuse the previous Key Pair by having the root CA certify it again for a new validity period.

5.7 Recovery following a compromise or disaster

5.7.1 Procedures for reporting and handling incidents and compromises

The CA takes appropriate technical and organizational measures (staff training, operational procedure guides, etc.) to manage the risks pertaining to the security of the trust services that are provided. These measures guarantee a security level that is commensurate with the degree of risk.

These measures are notably taken to prevent and mitigate the consequences of security-related incidents, and to inform the parties concerned of the detrimental effects of such incidents.

In the event of an incident, the OTU PKI refers to the CPTD and Worldline's Incident Management Policy [IMP] for reporting and processing. In addition, the OTU PKI takes the necessary measures, as far as possible, to avoid the recurrence of incidents as indicated in the Operational Security Policy [OSP].

5.7.2 Recovery procedures should IT resources (hardware, software or data) be corrupted

If the OTU PKI's equipment is damaged or out of order, and signature keys have not been destroyed, operation is restored as quickly as possible, the priority being given to the ability to provide the services for revoking and publishing the validity status of Certificates. Indeed, to ensure the continuous provision of its services, the OTU PKI has put in place a business continuity and recovery plan [BCRP].

An incident simulation test including a service interruption of an OTU PKI component is run regularly.

5.7.3 Recovery procedures if a component's private key is compromised

The situations in which an infrastructure key or an algorithm is compromised are handled via the incident management procedures, and the OTU PKI's BCRP. This plan is applied as soon as the OTU PKI becomes aware of the case.

This plan addresses the following points, among others, if the OTU CA's private key is compromised or is suspected of being compromised, if it is destroyed or if the algorithm used is compromised:

- After investigating the event, Worldline decides to revoke or not the OTU CA Certificate concerned.
- If it is decided to revoke the OTU CA Certificate concerned:
  - The OTU CA ensures the continuity of its services as described in the [BCRP].
  - All the Certificates issued by the OTU CA and signed with the private key concerned are revoked.
- If an algorithm is compromised, it is replaced.
- A new Key Pair is generated and a new corresponding CA Certificate is issued.
- Worldline decides on the communication plan intended for:
  - the Authorities that accredit the Certificate in question (Adobe...)
  - OTU CA Subscribers and Certificate Users

5.7.4 Disaster recovery

In the event of a disaster, the OTU PKI has the sufficient capacities needed to ensure the continuity of its services as defined in the BCRP. Following a disaster, this plan is put in place to restore the affected services.

5.8 End of the PKI's life

The OTU PKI does not transfer the OTU CA's activities to a third party.

If the OTU PKI decided to permanently end its activities, an activity cessation plan would then be applied. This plan includes the following points, among others:

- notification of the OTU PKI's decision to the persons concerned [inspection bodies such as ANSSI (*French National Cybersecurity Agency*), partners, Subscribers] before the cessation of its activities with a notice period;
- notification to Subscribers' representatives and the entities concerned of the upcoming revocation of the Certificate(s) which the OTU CA provided them with previously;
- revocation and management of the revocation status for the unexpired Certificates issued by the OTU CA;
- destruction of Key Pairs (primary ones and backups) and the related secrets;
- end of the contract with Subscribers;
- transfer of its obligations to Worldline.

The OTU PKI activity cessation plan is reviewed and updated regularly.

If the OTU PKI goes bankrupt, Worldline becomes responsible for meeting its end-of-life obligations.

6 Technical security measures

6.1 Key Pair generation and installation

6.1.1 Key Pair generation

In all the cases explained below, an entity's private key is always produced by the entity itself. Moreover, the transmission of private keys is completely prohibited.

6.1.1.1 CA keys

The OTU CA's Key Pairs are generated during a key ceremony. These key ceremonies take place

- within a physically isolated cryptographic module that meets the requirements defined in paragraph 6.2.1.1 of this document;
- on the OTU PKI's secure premises (see section 5.1);
- under the constant control of at least two (2) persons who have trusted roles within the OTU/PKI among secret holder, master of ceremony, HSM administrator and application manager (see subsection 5.2.1);
- in accordance with an organizational document and a technical document both signed by all participants, notably the master of ceremony.

The OTU CA's private key is used and kept on the OTU PKI's premises defined in chapter 5) of this document.

6.1.1.2 Authentication keys of a PKI component

The authentication keys of an OTU PKI component are generated during a key ceremony. These keys can be generated at the same time as the CA's keys. This ceremony takes place under the same conditions as those described in paragraph 6.1.1.1 above.

6.1.1.3 Subscriber's authentication keys

Subscriber authentication is described in subsection 3.2.5 of this CP/CPS.

The OTU PKI does not produce the Certificates associated with a Subscriber's private key and is not responsible for issuing these Certificates. Indeed, the Subscriber is informed of the rules that it must comply with to authenticate itself with the RA (see subsection 3.2.5), and it is its responsibility to obtain the Certificate (s) that enable it to authenticate itself with the RA.

6.1.1.4 Keys of the holder Certificates generated by the CA

The OTU CA does not generate the keys of holder Certificates.

6.1.1.5 Keys of the holder Certificates generated for the relying party

The Key Pairs are generated by the Certificate Holder Mechanism, which has exclusive use of them under the following conditions:

One-time-use Certificates	Organization Certificates
Within a physically isolated cryptographic module that meets the requirements defined in paragraph 6.2.1.1 of this document	

Copied to the other specific cryptographic modules intended for the same use, and which meet the same requirements as those mentioned above, in accordance with the cloning processes recommended by the supplier.	
On the OTU PKI's secure premises (see section 5.1)	
Under the control of the Certificate Holder Mechanism	Under the control of two (2) persons who have trusted roles within the OTU PKI
Following a script defined beforehand by the OTU CA	In accordance with an organizational document and a technical document both signed by all participants, notably the master of ceremony

The OTU PKI implements verification and protection methods in the Certificate Holder Mechanism to protect the use of the private keys.

In addition, this CP/CPS prohibits the use of an existing Key Pair associated with a former CSR.

6.1.2 Transmission of the private key to the beneficiary

Not applicable

6.1.3 Transmission of the public key to the CA

The Certificate Holder Mechanism sends the public key to the OTU CA in a template in PKCS#10 (CSR) format so the one-time-use Certificate or Organization Certificate is generated.

6.1.4 Transmission of the CA's public key to Certificate users

The Certificates containing the OTU CA's public keys are published on its website, the address of which is defined in section 2.2 of this document.

6.1.5 Key size

The size of the keys and the algorithms used comply with [ETSI TS 119 312] requirements.

Key Pairs	Algorithm	Hashing function	Size (bits)
OTU CA's Certificates	RSA	SHA-2	2,048
One-time-use Certificates	RSA	SHA-2	2,048
Organization Certificates	RSA	SHA-2	2,048
One-time-use Certificates for test purposes	RSA	SHA-2	2,048
Organization Certificates for test purposes	RSA	SHA-2	2,048

6.1.6 Verification of the generation of Key Pair settings and their quality

The OTU CA's Key Pairs are generated in accordance with the procedure described in paragraph 6.1.1.1 of this document. The settings of the equipment that generates the Key Pairs (HSM) are described in the organizational document of the key ceremony.

In the case of a one-time-use Certificate or an Organization Certificate, the characteristics of the Key Pair are verified by the OTU CA prior to any issuance of said Certificate.

6.1.7 Target uses of the key

The uses of the keys are defined in section 1.5, and more particularly within Certificates in accordance with the *Key Usage* extension (see section 7.1).

6.2 Security measures for the protection of private keys and for cryptographic modules

6.2.1 Security standards and measures for cryptographic modules

6.2.1.1 CA's cryptographic modules

The cryptographic modules (HSM) that the OTU PKI uses to generate the OTU CA's Key Pairs and the Key Pairs corresponding to the various Certificates issued by the OTU CA are certified cryptographic modules (HSMs) that meet the qualification requirements defined in subsection 6.2.11 of this document.

The OTU PKI ensures the security of the HSMs that it uses throughout their life cycle. Notably, procedures are implemented to

- ensure the integrity of these HSMs during their transportation,
- ensure the integrity of these HSMs during their storage, and
- ensure that these HSMs work properly.

6.2.1.2 Beneficiaries' cryptographic devices

Not applicable

6.2.2 Private key control

6.2.2.1 CA keys

The OTU CA's private keys and the corresponding backups are kept in a protected environment under the control of trusted staff—secret holders and system administrators (see subsection 5.2.1). This control is ensured by means of activation data that are called "secrets" and which are distributed among several persons with various trusted roles.

6.2.2.2 Holder Certificate keys

The private keys corresponding to the various Certificates issued by the OTU CA are under the exclusive control of the Certificate Holder Mechanism.

6.2.3 Private key escrow

Not applicable

6.2.4 Private key emergency backup

6.2.4.1 CA keys

The OTU CA's Key Pairs are backed up under the control of several persons during a key ceremony. The private keys are backed up

- on the OTU PKI's secure premises;
- under the constant control of at least two (2) persons who have trusted roles within the OTU PKI among secret holder, master of ceremony, HSM administrator and application manager (see subsection 5.2.1);
- using physically isolated hardware cryptographic resources (HSMs) that meet the requirements defined in paragraph 6.2.1.1 of this document;
- in accordance with the backup procedure described in the key ceremony technical document.

The backup procedures are executed in accordance with the specifications of the supplier of the OTU CA's HSMs.

The number of copies is limited to the minimum number required to ensure the continuity of the OTU PKI's services.

6.2.4.2 Holder Certificate keys

The private key of Organization Certificates is the only one for which an emergency backup is created during the Certificate creation ceremony. The backup is performed:

- on the OTU PKI's secure premises;
- under the control of two (2) persons who have a trusted role in the OTU PKI: secret holder and registration operator (see subsection 5.2.1);
- using physically isolated hardware cryptographic resources (HSMs) that meet the requirements defined in paragraph 6.2.1.1 of this document;
- in accordance with the backup procedure described in the key ceremony technical document.

The number of copies is limited to the minimum number required (2) to ensure the continuity of the OTU PKI's services.

6.2.5 Archiving of the private key

Not applicable

6.2.6 Transfer of the private key to or from the cryptographic module

6.2.6.1 CA keys

The OTU CA's private keys are generated in its HSM and are only transferred to another cryptographic module in the case of backup copies (see paragraph 6.2.4.1).

During a transfer, the private key is encrypted with an algorithm recommended by the HSM's manufacturer to ensure the security of information. The CA's encrypted private key cannot be decrypted without the use of hardware cryptographic components and the intervention of the persons who have the necessary trusted roles.

6.2.6.2 Holder Certificate keys

Not applicable

6.2.7 Storage of the private key into a cryptographic module

The OTU CA's private keys are stored in a physically isolated cryptographic module that meets the requirements defined in paragraph 6.2.1.1 of this document. The same goes for the storage of the backup copies of the OTU CA's private keys.

6.2.8 Private key activation methods

6.2.8.1 CA's private keys

The OTU CA's private keys can only be activated with activation data held by two (2) persons who have trusted roles within the OTU PKI.

A private key of the OTU CA can only be activated during a documented, traced key ceremony.

6.2.8.1 Private keys of one-time-use Certificates

The private keys of one-time-use Certificates are activated by the Certificate Holder Mechanism using one of the cryptographic modules intended for this use, after the receipt of the one-time Certificate issued by the OTU CA during the signing session.

6.2.8.2 Private keys of Organization Certificates

The private keys of Organization Certificates are activated by the Certificate Holder Mechanism in one of the cryptographic modules intended for this use, after the receipt of a duly validated, authenticated request.

6.2.9 Private key deactivation method

6.2.9.1 CA's private keys

The OTU CA's private keys stored in the HSM are automatically deactivated as soon as the latter is stopped or disconnected.

6.2.9.2 Private keys of one-time-use Certificates

The private key of a one-time-use Certificate is destroyed after use.

6.2.9.3 Private keys of Organization Certificates

The private key of an Organization Certificate is automatically deactivated in the cryptographic module at the end of the signing operation session or as soon as the module is stopped or disconnected.

6.2.10 Private key destruction method

6.2.10.1 CA's private keys

The OTU CA's private keys and the corresponding backup copies are destroyed through deletion in the hardware cryptographic resource. Destruction operations are carried out during an audited, Key Ceremony-type procedure.
Destroying the OTU CA's private keys or the corresponding backup copies in the HSM requires that the keys present in the hardware cryptographic module be destroyed. The reset functions specific to the module are then used so no information can be used to restore these private keys, even partially. If the functions needed to destroy the OTU CA's keys are inaccessible or no longer accessible in the HSM, the latter is destroyed physically.

When one of the OTU CA's private keys reaches the end of its life, normally or early (because of revocation), it is systematically destroyed, as well as any copy and element that makes it possible to reconstitute it. Moreover, in the case where the hardware cryptographic resource hosting the OTU CA's private keys must be decommissioned, then these keys are as well.

6.2.10.2 Private keys of one-time-use Certificates

The private keys of one-time-use Certificates are destroyed after use by the Certificate Holder Mechanism which then logs the event.

6.2.10.3 Private keys of Organization Certificates

Not applicable

6.2.11 Certification of the cryptographic module

The hardware cryptographic module used to host the OTU CA's private keys is evaluated at the following Certification level: Common Criteria EAL4+.

The hardware cryptographic module used to host the private keys of the holder Certificates generated by the OTU CA is evaluated at the following Certification level: FIPS 140-2 level 2.

6.3 Other aspects of Key Pair management

6.3.1 Archiving of public keys

The OTU CA's public keys are archived in accordance with paragraph **Erreur ! Source du renvoi introuvable.** of this document.

6.3.2 Life spans of Key Pairs and Certificates

The life spans of Key Pairs and Certificates vary according to the type of Certificate. The size of Key Pairs was taken into account when defining these life spans, in accordance with [ETSI TS 119 312] cryptographic requirements.

The OTU CA may not issue holder Certificates whose life spans exceed that of the OTU CA Certificate used for the issuance.

Key Pairs	Life span
OTU CA's Certificates	10 years
One-time-use Certificates	15 minutes
Organization Certificates	3 years
One-time-use Certificates for test purposes	15 minutes
Organization Certificates for test purposes	3 years

6.3.3 Key inventory

The OTU CA makes an inventory to make sure that all the private keys that it has produced for the Certificate Holder Mechanism were requested properly.

6.4 Activation data

6.4.1 Generation and installation of activation data

6.4.1.1 Generation and installation of the activation data corresponding to the CA's private key

The activation data of the OTU CA's private keys are generated in a Hardware Security Module (see paragraph 6.2.2.1) during key ceremonies under the control of two (2) persons who have trusted roles. These activation data are stored on smart cards and then handed to the secret holders who then possess them (see paragraph 6.2.8.1). The officers identified by name as part of the trust roles assigned to them are the only persons to know these activation data.

6.4.1.2 Generation and installation of the activation data corresponding to the private key of the holder Certificate

Not applicable

6.4.2 Protection of activation data

6.4.2.1 Protection of the activation data corresponding to the CA's private key

The activation data are protected by cryptographic and physical access control mechanisms. Secret holders are in charge of protecting the secrets which they are responsible for. A secret holder does not hold more than one CA activation datum.

6.4.2.2 Protection of the activation data corresponding to the private key of the holder Certificate

The authentication system of the Certificate Holder Mechanism is protected, both for the activation and use of the private keys.

6.5 IT systems security measures

6.5.1 Technical security requirements specific to IT systems

The minimum technical security requirements implemented by the OTU PKI meet the following objectives:

- identification and strong authentication of users for accessing the system;
- use session management: disconnection after idle time, file access restrictions based on roles and usernames;
- protection against computer viruses and all forms of malicious or unauthorized software; software updates;
- management of users' accounts and rights;
- protection of the network against any intrusion by an unauthorized person;
- protection of the network to ensure the confidentiality and integrity of the data transmitted through it;
- audit functions: non-repudiation, accountability, and nature of the actions performed;
- application of change procedures for actions of delivery, modification and urgent resolution of software problems;
- application of change procedures for any change made to software configurations;
- redundancy of network connections to ensure accessibility in the event of a simple malfunction.

The following measures are also implemented:

- monitoring mechanisms with automatic alerts and recording;

- procedures for auditing system settings, particularly routing settings; and
- incident handling procedures.

6.5.2 Qualification of IT systems

Not applicable

6.6 Security measures for systems throughout their life cycles

6.6.1 Security measures with regard to system development

The implementation, configuration and any modification or update of a system used to implement the PKI's components are documented and monitored.

6.6.2 Security management measures

Any change made to the system of an OTU PKI component is documented and traced. It appears in the internal functioning procedures of the component concerned.

6.6.3 Evaluation of the security of systems' life cycles

Not applicable

6.7 Network security measures

The OTU PKI is not in direct contact with open networks. The access gateways are protected against intrusion or attack attempts.
Penetration tests are run during the installation of the infrastructure, and with each major upgrade or modification. Vulnerability tests are run regularly.
These gateways restrict open services and protocols to the services that the OTU PKI imperatively needs in order to function. They are regularly updated to take into account the changes in anti-intrusion systems and to fix potential security holes as soon as they are identified by the community of network users.

System configuration is carried out by removing unused accounts, applications, services, protocols, and ports.

The critical network components are maintained in a secure environment, and their configurations are periodically audited so they remain compliant with the requirements specified by this CP/CPS.

The Root CA is stored in a highly secure area and is only woken up when necessary.

6.8 Timestamping system

The events are timestamped with the system time of the OTU PKI's servers. The clocks of the OTU PKI's systems are synchronized with one another using a reliable (UTC) time source every 24 hours.

7 Certificate, OCSP and CRL profiles

7.1 Certificate profiles

7.1.1 Definitions

The Certificates that the OTU CA issues, including its own, comply with X.509 standards.

Fields	Description
Version	X.509 Certificate Version
Serial number	Unique serial number of the Certificate
Signature	OID of the algorithm used by the issuer CA to sign the issued Certificate
Issuer	Value of the DN (X.500) of the CA that issues the Certificate
Validity	Activation and expiry dates of the Certificate
Subject	Value of the DN (X.500) of the Subject
Subject Public Key Info	OID of the algorithm and value of the public key
Extensions	Extension list An extension can be critical or non-critical: • If the extension is critical, the user application which the Certificate is submitted to must be able to handle it in accordance with its use. If the application cannot handle the extension, or if the extension does not conform to the use that the application expects, the latter must reject the Certificate. • If it is non-critical, Certificates are not rejected, and the application is allowed to ignore the extension in question.

7.1.2 OTU CA's Certificates

The OTU CA's Certificates, which are called Technical CA (TCA) Certificates, are differentiated by the *Serial Number* (SERIALNUMBER) field of the *Distinguished Name* (DN) of the *Subject*.

DN fields	Mandatory	Description
C	Yes	Country of the Organization governing the CA: FR
O	Yes	Legal name of the Organization governing the CA: Worldline
OU	Yes	Identifier of the Organization governing the CA: 0002 378901946
SERIALNUMBER	Yes	Unique serial number of the DN [1]
CN	Yes	Subject's identity: OTU CA

7.1.2.1 Fields and basic values

Fields	Value
Version	V3 (value: 2)
Serial number	Generated automatically during the Key Ceremony
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	DN of the Root CA
Validity	10 years
Subject	DN of the Technical CA (see chapter 0)
Subject Public Key Info	RSA, 2,048 bits

7.1.2.2 Certificate extensions

Fields		Critical	Value
Authority Key Identifier		No	[RFC 5280] method [0]: identifier of the issuer CA's public key
Subject Key Identifier		No	[RFC 5280] method [1]: identifier of the public key contained in the Certificate
Key Usage		Yes	keyCertSign, CRLSign
Basic Constraint	Certification Authority	No	true
	Maximum Path Length		0
Certificate Policies	policyIdentifier	No	anyPolicy (2.5.29.32.0)
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		No	Not used
Issuer Alternative Name		No	Not used
CRL Distribution Points		No	http://root.mediacert.com/LatestCRL[2]
Authority Information Access		No	Not used

[1] This SERIALNUMBER is used to differentiate the various TCAs. It is a counter that is incremented upon each issuance of a new TCA. It is constructed as follows:

SERIALNUMBER =

- *1:* represents Technical Certification Authority 1.
- *2:* represents Technical Certification Authority 2.
- …

[2] This URL is given for informational purposes. The URL that prevails is the one contained in the Certificate.

7.1.3 One-time-use Certificates

7.1.3.1 Basic fields

Fields		Value
Version		V3 (value: 2)
Serial number		Defined by the issuer Technical CA
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN of the issuer Technical CA
Validity		15 minutes
Subject	C	Subject's nationality
	SN	Subject's name
	GN	Subject's forename
	OU	Subscriber's name
	SERIALNUMBER [3]	Unique serial number of the DN
	CN	Subject's identity in this format: Subject's Forename [space] Subject's Surname [space] [TraceID] [4]
Subject Public Key Info		RSA, 2,048 bits

7.1.3.2 Certificate extensions

Fields		Critical	Value
Authority Key Identifier		No	[RFC 5280] method [0]: identifier of the issuer CA's public key
Subject Key Identifier		No	[RFC 5280] method [1]: identifier of the public key contained in the Certificate
Key Usage		Yes	nonRepudiation
Basic Constraint	Certification Authority	No	False
Certificate Policies	policyIdentifier	No	1.2.250.1.111.17.0.3.1
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		No	Not used
Issuer Alternative Name		No	Not used
Extended Key Usage		No	Not used
CRL Distribution Points		No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/crl [5]
Authority Information Access	ocsp	No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/ocsp [5]
	caIssuers		http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/certificate [5]

[3] In accordance with [RFC 3739], the SERIALNUMBER field makes it possible to eliminate the risk of homonymy in the rest of the DN fields. It is built as follows:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime* represents the time at which the Certificate was requested.
- *DocRef* represents the identifier of the document to sign (If several documents must be signed, the first document referenced in the signing request is used.).
- *ClientId* represents the client's unique identifier.

The *ReqTime* value is useful for the case where two (2) persons bearing the same name sign a document jointly. The concatenation of these three (3) pieces of information guarantees a unique value among all users.

[4] represents the unique identification of the trace container for the signature.

[5] This URL is given for informational purposes. The URL that prevails is the one contained in the Certificate.

7.1.4 Organization Certificates

7.1.4.1 Basic fields

Fields		Value
Version		V3 (value: 2)
Serial number		Defined by the issuer Technical CA
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN of the issuer TCA
Validity		3 years
Subject	C	Organization 's country
	OI [6]	Organization's identifier in this format: ICD [space] Organization's identifier
	SN [7]	Surname of the authorized individual in the Organization
	GN [7]	Forename of the authorized individual in the Organization
	OU [7]	Name of the unit in the Organization
	OU	Subscriber's name
	SERIALNUMBER [8]	Unique serial number of the DN
	CN	Organization's identity
Subject Public Key Info		RSA, 2,048 bits

7.1.4.2 Certificate extensions

Fields		Critical	Value
Authority Key Identifier		No	[RFC 5280] method [0]: identifier of the issuer CA's public key
Subject Key Identifier		No	[RFC 5280] method [1]: identifier of the public key contained in the Certificate
Key Usage		Yes	nonRepudiation
Basic Constraint	Certification Authority	No	False
Certificate Policies	policyIdentifier	No	1.2.250.1.111.17.0.3.2
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		No	[RFC 822]: Certificate Subject's e-mail address
Issuer Alternative Name		No	Not used
Extended Key Usage		No	Not used
CRL Distribution Points		No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/crl [9]
Authority Information Access	ocsp	No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/ocsp [9]
	caIssuers		http://pki-otu-ac[SERIALNUMBER of issuer

[6] The ICD (*International Code Designator*) is a unique 4-character code, and the Organization's ID consists of 35 characters at most. For Organizations governed by French law, the ICD is 0002, and the accepted Organization identifier is the SIREN number.
[7] At least one of these two pieces of information must be present in the DN: the name of the unit in the Organization, or the forename and surname of the individual authorized to represent the Organization.
[8] In accordance with [RFC 3739], the SERIALNUMBER field makes it possible to eliminate the risk of homonymy in the rest of the DN fields. It is built as follows:

SERIALNUMBER = *CreationDate*

- *CreationDate* represents the date and time (arbitrary) at the moment on which the Certificate was withdrawn. It uses the *yyyymmddhhmmss* format.

The *CreationDate* value is useful for the case where two (2) persons bearing the same name sign a document jointly. The concatenation of these two (2) pieces of information guarantees a unique value among all users.
[9] This URL is given for informational purposes. The URL that prevails is the one contained in the Certificate.

			TCA].mediacert.com/certificate [9]

7.1.5 One-time-use Certificate for test purposes

7.1.5.1 Basic fields

Fields		Value
Version		V3 (value: 2)
Serial number		Defined by the issuer Technical CA
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN of the issuer TCA
Validity		15 minutes
Subject	C	Subject's nationality
	SN	Subject's name
	GN	Subject's forename
	OU	Subscriber's name
	SERIALNUMBER [10]	Unique serial number of the DN
	CN	Test Subject's identity in this format: TEST [space] Subject's Forename [space] Subject's Surname [space] [TraceID] [11]
Subject Public Key Info		RSA, 2,048 bits

7.1.5.2 Certificate extensions

Fields		Critical	Value
Authority Key Identifier		No	[RFC 5280] method [0]: identifier of the issuer CA's public key
Subject Key Identifier		No	[RFC 5280] method [1]: identifier of the public key contained in the Certificate
Key Usage		Yes	nonRepudiation
Basic Constraint	Certification Authority	No	False
Certificate Policies	policyIdentifier	No	1.2.250.1.111.17.0.3.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		No	Not used
Issuer Alternative Name		No	Not used
Extended Key Usage		No	Not used
CRL Distribution Points		No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/crl [12]
Authority Information	ocsp	No	http://pki-otu-ac[SERIALNUMBER of issuer

[10] In accordance with [RFC 3739], the SERIALNUMBER field makes it possible to eliminate the risk of homonymy in the rest of the DN fields. It is built as follows:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime* represents the time at which the Certificate was requested.
- *DocRef* represents the identifier of the document to sign (If several documents must be signed, the first document referenced in the signing request is used.).
- *ClientId* represents the client's unique identifier.

The *ReqTime* value is useful for the case where two (2) persons bearing the same name sign a document jointly. The concatenation of these three (3) pieces of information guarantees a unique value among all users.

[11] represents the unique identification of the trace container for the signature.

[12] This URL is given for informational purposes. The URL that prevails is the one contained in the Certificate.

Access			TCA].mediacert.com/ocsp [12]
	calssuers		https://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/certificate [12]

7.1.6 Organization Certificate for test purposes

7.1.6.1 Basic fields

Fields		Value
Version		V3 (value: 2)
Serial number		Defined by the issuer Technical CA
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN of the issuer TCA
Validity		3 years
Subject	C	Organization 's country
	OI [13]	Organization's identifier in this format: ICD [space] Organization's identifier
	SN [14]	Surname of the authorized individual in the Organization
	GN [14]	Forename of the authorized individual in the Organization
	OU [14]	Name of the unit in the Organization
	OU	Subscriber's identity
	SERIALNUMBER [15]	Unique serial number of the DN
	CN	TEST Organization's identity [16]
Subject Public Key Info		RSA, 2,048 bits

7.1.6.2 Certificate extensions

Fields		Critical	Value
Authority Key Identifier		No	[RFC 5280] method [0]: identifier of the issuer CA's public key
Subject Key Identifier		No	[RFC 5280] method [1]: identifier of the public key contained in the Certificate
Key Usage		Yes	nonRepudiation
Basic Constraint	Certification Authority	No	False
Certificate Policies	policyIdentifier	No	1.2.250.1.111.17.0.3.4
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		No	[RFC 822]: Certificate Subject's e-mail address
Issuer Alternative Name		No	Not used
Extended Key Usage		No	Not used
CRL Distribution Points		No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/crl [17]
Authority Information Access	ocsp	No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/ocsp [17]

[13] The ICD (*International Code Designator*) is a unique 4-character code, and the Organization's ID consists of 35 characters at most.
For Organizations governed by French law, the ICD is 0002 and the accepted Organization identifier is the SIREN number.
[14] At least one of these two pieces of information must be present in the DN: the name of the unit in the Organization, or the forename and surname of the individual authorized to represent the Organization.
[15] In accordance with [RFC 3739], the SERIALNUMBER field makes it possible to eliminate the risk of homonymy in the rest of the DN fields. It is built as follows:

SERIALNUMBER = *CreationDate*

- *CreationDate* represents the date and time (arbitrary) at the moment on which the Certificate was withdrawn. It uses the *yyyymmddhhmmss* format.

The *CreationDate* value is useful for the case where two (2) persons bearing the same name sign a document jointly. The concatenation of these two (2) pieces of information guarantees a unique value among all users.
[16] The word "TEST" and the Organization's identity are not separated by a space.
[17] This URL is given for informational purposes. The URL that prevails is the one contained in the Certificate.

	caIssuers		http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/certificate [17]

7.2 CRL profile

7.2.1 Basic fields

Fields		Value
Version		V2 (value: 1)
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN of the issuer TCA
This Update		CRL issuance date
Next Update		CRL issuance date + 7 days [18]
Revoked Certificates	userCertificate	Unique serial number of the revoked Certificate
	revocationDate	Revocation date
	crlEntryExtensions	Additional information that can be provided in CRL entry extensions

7.2.2 CRL extensions

Fields	Critical	Value
Authority Key Identifier	No	[RFC 5280] method [0]: identifier of the issuer TCA's public key
CRL Number	No	Number of the CRL defined by the issuer Technical CA
Issuer Alternative Name	No	Not used
Delta CRL Indicator	Yes	Not used
Fresh CRL	No	Not used

7.2.3 CRL entry extensions

Fields	Critical	Value
Reason Code	No	[RFC 5280]: code corresponding to the correct reason for the revocation
Invalidity Date	No	Not used
Certificate Issuer	No	Not used

[18] In the case where the OTU CA's activity ends permanently, the last published CRL is valid for three (3) years.

7.3 OSCP profile

In accordance with subsection 4.10 of this document, the OTU PKI provides users with an OCSP responder so they can check in real time the status of the Certificates issued by the OTU CA. This service complies with [RFC 6960]. In this context, the OCSP responder has a Certificate that is issued by the OTU CA and whose profile is detailed below.

7.3.1 Basic fields

Fields		Value
Version		V3 (value: 2)
Serial number		Defined by the issuer Technical CA
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN of the issuer TCA
Validity		3 years
Subject	C	FR
	OI	0002 378901946
	OU	OTU CA
	O	Worldline
	SERIALNUMBER [19]	Unique serial number of the DN
	CN	OTU PKI's OCSP Service
Subject Public Key Info		RSA, 2,048 bits

7.3.2 Certificate extensions

Fields		Critical	Value
Authority Key Identifier		No	[RFC 5280] method [0]: identifier of the issuer CA's public key
Subject Key Identifier		No	[RFC 5280] method [1]: identifier of the public key contained in the Certificate
Key Usage		Yes	Digital Signature
Basic Constraint	Certification Authority	No	False
Certificate Policies	policyIdentifier	No	1.2.250.1.111.17.0.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		No	Not used
Issuer Alternative Name		No	Not used
Extended Key Usage		No	ocspSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/crl
Authority Information Access	ocsp	No	http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/oscp[20]
	caIssuers		http://pki-otu-ac[SERIALNUMBER of issuer TCA].mediacert.com/certificate [20]

[19] In accordance with [RFC 3739], the SERIALNUMBER field makes it possible to eliminate the risk of homonymy in the rest of the DN fields. It is built as follows:
SERIALNUMBER = number incremented each time an OCSP Certificate is issued for the relevant issuer Technical CA

[20] This URL is given for informational purposes. The URL that prevails is the one contained in the Certificate.

8 Compliance audit and other evaluations

8.1 Frequency and/or circumstances of audits

Worldline has an approved firm audit the compliance with the CP/CPS in force during the operational implementation of a component of the OTU PKI, and during any significant change within a component.

Every two years, Worldline has an approved firm carry out an external Certification audit of the OTU PKI in the [ETSI EN 319 411-1] standard.

In addition, Worldline carries out an internal monitoring audit between two external certification audits in the [ETSI EN 319 411-1] standard.

8.2 Auditors' identities and qualifications

8.2.1 External audit

The component is audited by a team of auditors who are part of an approved audit firm authorized to carry out audits in accordance with the specifications of [ETSI EN 319 411-1].

8.2.2 Internal audit

The component is audited out by a team independent of the OTU PKI and in charge of compliance checks.

8.3 Relationships between auditors and audited entities

8.3.1 External audit

The auditor(s) who audit the OTU PKI's component(s) must be independent and free from any conflict of interest.

8.3.2 Internal audit

The auditor(s) who audit the OTU PKI's component(s) must not have any trusted role within the PKI component being audited.

8.4 Subjects covered by audits

The audits carried out by auditors cover all or part of the OTU PKI's components. They aim to verify whether this CP/CPS is correctly implemented, and whether the OTU CA's procedures and practices comply with the requirements which it is subjected to.

In this regard, before each audit, the auditor in charge of the audit sends the OTU PKI an audit plan that specifies the components and procedures that they plan to audit with their colleague(s), and the detailed agenda of the audit.

8.5 Actions carried out following audit conclusions

After an audit, the audit team gives Worldline one of the following results:

- success: no nonconformities have been found, and no new action is required. Worldline confirms that the audited component complies with the obligations expressed in this document and with the announced practices.

- to be confirmed: one or more non-blocking nonconformities have been identified. Worldline must then submit a corrective action plan with a deadline for its completion. A new audit may be carried out to verify the implementation of the corrections.

- failure: one or more blocking nonconformities have been identified. The audit team then makes recommendations to Worldline, which may be a temporary or permanent cessation of activity, revocation of the CA's Certificate, etc. The choice of the measure to apply is left to Worldline.

8.6 Publication of results

The results of conformity audits are made available to the Certification body in charge of the certifying the OTU PKI.

9 Other business and legal issues

9.1 Prices

Worldline does not market its Certificates alone, but only through higher-level services.

9.1.1 Prices for the supply or renewal of Certificates

This is addressed in the higher-level service provision contract that exists between Worldline and the Subscriber.

9.1.2 Prices for accessing Certificates

This is addressed in the higher-level service provision contract that exists between Worldline and the Subscriber.

9.1.3 Prices for accessing Certificate status and revocation information

Not applicable

9.1.4 Prices for other services

Not applicable

9.1.5 Refund policy

Not applicable

9.2 Insurance

9.2.1 Insurance coverage

Worldline has taken out, with a notoriously solvent insurance company, an insurance policy that guarantees the potential damage to its property and staff, and a policy covering its professional liability as part of the services provided.

9.2.2 Other resources

Worldline has the financial resources needed to provide the OTU PKI's services.

9.2.3 Coverage and guarantee applicable to user entities

Not applicable

9.3 Professional data confidentiality

9.3.1 Scope of confidential information

The following information is considered as confidential:

- the technical information pertaining to the security of the inner workings of the PKI's cryptographic modules and some of the PKI's components;
- the private keys of the OTU CA, its components and the issued Certificates;
- the activation data of the OTU CA's private keys;
- the CPTD;
- the internal operation procedures;
- the BCRP;
- the activity cessation plan;
- event logs;
- registration files;
- audit reports.

Only the persons that have been authorized by Worldline, and have the need and authorization to know its content may view the aforementioned confidential information on demand. This request must be forwarded to the head of the OTU CA or to one of their deputies who will approve or not request that has been submitted to them.

9.3.2 Non-confidential information

The information of the OTU PKI that is considered public and therefore non-confidential is made accessible as defined in section 2.2 of this document.

9.3.3 Responsibilities with regard to the protection of confidential information

9.3.3.1 Applicable legislation

Worldline processes personal data in accordance with the French personal data protection legislation in force on the French territory, which conforms to that which prevails on the European territory. Worldline takes all the appropriate and necessary measures in accordance with these regulations so the personal data that it is required to keep via the OTU PKI are protected from any compromise, security breach or loss of integrity that could have significantly affect the trust service provided and the personal data stored there.

To this end, the OTU PKI notably implements the security measures of the premises and information systems to prevent the files in its possession from being altered, damaged, or accessed by unauthorized third parties.

9.3.3.2 Prior consent of the Subject, Organization representatives and Subscriber representatives to the processing of their data by the OTU PKI

Some personal data must be collected as part of the creation of registration files. They are sent to the RA of the OTU PKI by the Subscribers or their representatives.

9.3.3.2.1 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, before any request initiated on their behalf by the Subscriber, that their personal data, sent by the Subscriber to 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;
- 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.

The future Subject's consent to this processing, as part of the implementation of the electronic signature, must be expressed by means of a positive action by said Subject, who has been informed beforehand of the consequences of their choice and has the means to exercise it.

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 CA, via the RA and at the latter's request, retains 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.

9.3.3.2.2 Organization Certificates

For the constitution of the registration file, the Subscriber, via its representatives, provides the RA with the necessary personal data. The Subscriber's representative performs this transmission knowing the purposes associated with this data collection. For this purpose, the Subscriber's representatives and the possible representatives of the Organization will have to accept that their personal data undergo computer processing for the sole purposes of

- constituting their identification and, in the case where the Subscriber and the Organization are the same entity, making their authentication possible in order to generate a Certificate containing their information;
- backing up the identity that might be specified in the Certificate and the powers vested by providing necessary evidence, if need be, through the retention of the elements in the Evidence file.

Consequently, the Subscribers' representatives, by agreeing to represent the Subscribers, accept that their personal data are processed and kept for as long as required by the purposes of the processing operations carried out as part of the delivery and management of Organization Certificates.

9.3.3.3 Right of access to data

In accordance with Article 40 of the French Data Protection Act, amended by Law No. 2016-1321 of 7 October 2016 - art. 63. "Any natural person proving their identity may require that a data processing officer, depending on cases, rectify, complete, update, lock or erase the personal data that concern them and which are inaccurate, incomplete, ambiguous, outdated; or whose collection, use, disclosure or storage is prohibited. When the person in question requests it, the processing officer must provide proof, at no cost for the requisitioner, that they have carried out said operations.

Consequently, the persons who consented beforehand to the processing of their personal data by the OTU PKI as stated above may, under the law, access all the information about them kept by the RA and obtain a copy thereof.

However, regarding one-time-use Certificates, the personal data used to back up the Subject's identification for the production of the Certificate with which they have signed can only be locked or deleted when the purpose for which said personal data were collected and processed has been completed. The same applies to the personal data of Subscribers' representatives and Organization representatives, which must be maintained and kept by the RA for the duration defined in subsection 5.5.2 of this document.
In addition, the same personal data may be rectified, completed or updated at the request of the person concerned by these data, provided that the personal data used to identify and authenticate this person, which were supplied during the electronic signature process or the constitution of the registration file, remain in the trace history of the transaction and of the electronic signature carried out, or of the Organization Certificate creation request, until the purpose for which said personal data were collected and processed has been met.

These reservations constitute a restriction on the rights provided for in Article 40 and are based on the purposes that justify the processing of these data as part of the provision of trust services.
The OTU PKI is not allowed to use any of the personal data transmitted during the registration of the Subject or during the constitution of the registration file for Subscribers and Organizations for a purpose other than that defined in the CP/CPS.

The right of access can be exercised in writing through the following methods: by postal mail to the OTU CA's point of contact whose address is given in subsection 1.6.2 of this document or on the OTU CA's website (see section 2.2), accompanied by a copy of an identity document. Ideally, this mail should be registered mail with an acknowledgment of receipt.

9.3.3.4 Conditions under which personal information is disclosed to legal or administrative authorities

Worldline may have to make the registration files of Subjects, Subscribers and Organizations available to authorized third parties as part of legal proceedings or audits that aim to verify the delivery of Certificates. The OTU PKI has secure procedures to allow this access, the occurrences of which are traced by name and kept.

9.4 Personal data protection

9.4.1 Personal data protection policy

Worldline ensures the protection of the personal data that it has or may have in its possession, in accordance with the aforementioned rules pertaining to the protection of personal data in force in the territory from which it provides its services.

For this purpose, the OTU PKI's RA collects and processes the identification data of future Subjects, Subscribers' contacts or representatives, and Organizations' contacts or representatives contained in the registration files (evidence file) as personal information.

These data are protected in accordance with the French national law applicable to its services which, in France, complies with European regulations.

Thus, in accordance with the eIDAS regulation, the OTU PKI takes the appropriate technical and organizational measures to manage the risks pertaining to the security of the trust services that it provides. Given the latest technological developments, these measures ensure that the level of security is commensurate with the degree of risk. Notably, measures are taken to prevent and mitigate the consequences of security-related incidents, and to inform the parties concerned of the detrimental effects of such incidents.

In the event of a personal data breach, the OTU PKI refers to Worldline's Personal Data Breach Handling Procedure [PDBHP], which is at its disposal.

The OTU PKI undertakes to implement the Operational Security Policy [OSP] in force, and acts in accordance with LRC (Legal, Regulatory and Contractual) obligations.

9.4.2 Personal information

The registration data of the Subject or authorized Individuals supplied by the Subscriber are considered as personal information.

9.4.3 Non-personal information

Not applicable

9.4.4 Responsibilities with regard to the protection of personal data

The OTU PKI acts in accordance with the legislation and regulations defined in subsection 9.4.1 of this document.

9.4.5 Use of personal data - Notification and consent

The OTU PKI acts in accordance with the legislation and regulations defined in subsection 9.4.1 of this document. The information that any Subscriber gives to the RA is protected against disclosure without the consent of the Subscriber and of the persons who have mandated it to give such information to the OTU PKI.

9.4.6 Conditions under which personal information is disclosed to legal or administrative authorities

The OTU PKI acts in accordance with the legislation and regulations defined in subsection 9.4.1 of this document.

9.4.7 Other circumstances under which personal information is disclosed

Not applicable

9.5 Intellectual and industrial property rights

The OTU PKI acts in accordance with the legislation and regulations defined in subsection 9.4.1 of this document. Public documents, which fall outside the scope of confidential information, remain the property of Worldline.

9.6 Contractual interpretations and guarantees

The various components of the OTU PKI must ensure

- the protection (integrity and confidentiality) of their private keys and possibly of their activation data throughout their life cycle;
- the use of Key Pairs and Certificates for the uses for which they were issued, in accordance with the applications defined in section 1.5 of this CP/CPS;
- that this CP/CPS is implemented and complied with;
- that they will undergo the compliance audits carried out by external auditors, and will implement the resulting recommendations;
- that the technical and human resources needed to honor commitments will be implemented, notably with regard to the specified service level;
- that internal functioning procedures are documented;
- that its policies and procedures do not contain any discriminatory practices.

9.6.1 CA

The OTU CA must

- make sure that the RA acting on behalf of the OTU CA complies with this CP/CPS;

- publish the public information listed in section 2.2 of this document, and notably the GTOS and the TS, in a durable, secure way;
- guarantee the compliance with the OSP of the OTU PKI by the latter's various components;
- make its services available to any Subscriber that has accepted the GTOS;;
- collaborate with auditors during compliance audits and implement any actions that might be decided with auditors following these audits.

9.6.2 RA

The RA must

- comply with the Registration procedures described in this CP/CPS.

9.6.3 Certificates beneficiaries

Certificate beneficiaries must

- protect the means of access to private keys and Certificates;
- only use their Certificates for the uses provided for and defined in the associated CP/CPS;
- revoke their Certificate or have it revoked if it is compromised or suspected of being compromised;
- revoke their Certificate or have it revoked if the means of access are compromised or suspected of being compromised;
- verify and meet the obligations incumbent upon them as described in this document and in TS.

9.6.3.1 Subscriber

In addition to the obligations defined in subsection 9.6.3, the Subscriber has the following obligations, which vary according to the type of Certificate.

9.6.3.1.1 One-time-use Certificates

For a one-time-use Certificate, the OTU CA Subscriber must

- collect and verify, or have someone collect and verify, under its own responsibility, the identity information given by the future Subject;
- inform the Subject of their obligations; see paragraph 9.6.3.2;
- inform the Subject about the Certificate request process and the consequences of using the Certificate, in accordance with this CP/CPS;
- provide, in its request, the data pertaining to the identification of the future Subject as well as the latter's necessary consent as defined in paragraph 3.2.3.1 of this document;
- draw up and sign the future Subject's Certificate request;
- keep exclusive control over the methods that it uses to authenticate itself with the OTU PKI's RA;

- inform the RA as early as possible of any event that might be detrimental to the quality of the identification of its future Subjects;

- 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;

- have non-discriminatory practices.

9.6.3.1.2 Organization Certificates

For an Organization Certificate, the OTU CA Subscriber must

- complete the Certificate request file by supplying all the required elements, and the necessary supporting documents and authorizations (see paragraph 4.1.2.2). The information and supporting documents given to the RA during the Certificate creation request must be accurate, truthful and up to date.

- inform the RA if the Certificate's data become invalid because of a change in the Organization. To do so, the Organization must send the following information to the RA immediately by means of registered mail with acknowledgment of receipt:

    - 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.

- request the revocation of the Certificate in the situations listed in this document. In this regard, the change in the information appearing in an Organization Certificate entails the revocation of the Certificate and its replacement at the Organization's expense.

- inform the RA as quickly as possible of any event that might affect the reliability of the means that it uses to authenticate itself with said Authority. In this regard, the changes (forename, last name, e-mail address) must be notified to the RA.

- inform the RA should the Organization no longer exist. In this regard, 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.

- 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 regard, the Subscriber must inform the RA as soon as possible, through a simple letter, of the changes in the information.

- have non-discriminatory practices.

If the Subscriber resorts to a technical service provider, it is its responsibility to have the latter meet these obligations, all the more so since this provider may hold secrets specific to the Subscriber such as the private keys corresponding to authentication and message signing Certificates. It is the Subscriber's responsibility to make sure that appropriate measures are taken to protect the access to these secrets.

9.6.3.2 Subject

In addition to the obligations defined in subsection 9.6.3, the future Subject must give the information and supporting documents requested by the Subscriber, and which they certify as accurate and up to date during the Certificate request.

The obligations incumbent upon the future Subject are also defined in the contract signed with their agent, who is here referred to as the Subscriber.

9.6.4 Certificate users

The users of the Certificates provided by the OTU CA must

- verify and meet the obligations incumbent upon them as per this document and the TS. For one-time-use Certificates, these obligations will be described by the Subscriber in the contract that binds them to the future Subject. This contract sets out how an electronic signature works, what this choice entails, how to perform it and collect the required consent in accordance with the clauses of its Subscription Contract.
- verify the use for which a Certificate has been issued, and comply with it;
- verify the validity of the Certificate (expiry, revocation, integrity) and that of each Certificate of the Certification Chain.

9.6.5 Other participants

9.6.5.1 Security Committee

The Safety Committee must, among other things:

- read and master the complete documentation of the OTU PKI;
- ensure and maintain the consistency of this CP/CPS;
- validate the OSP and the Risk Analysis of the OTU PKI.

9.7 Limited guarantee

The OTU CA undertakes to issue Certificates in accordance with this document and the state of the art.

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 the verified request of a Subscriber authenticated 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.

No other guarantee is provided.

9.8 Limited liability

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

The OTU CA may in no case whatsoever be held liable in the event of a fault occurring within the scope of a Subscriber entity, and notably:

- the use of an expired Certificate,
- the use of a revoked Certificate, or

- the use of a Certificate for a use other than those described in section 4.5 of this CP/CPS.

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

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

9.9 Compensation

The OTU CA delivers Certificates as part of higher-level electronic services, notably electronic subscription services.

The framework agreement signed between the customer and Worldline or its duly authorized agent sets out the clauses with regard to compensation should damage occur. If there is no framework agreement, Worldline's GTS will be applicable.

9.10 Validity period and early expiry of the CP

9.10.1 Validity period

This CP/CPS becomes effective when it is published on the OTU PKI's website at the end of the notice period (see section 9.11), after having been validated by the entity that manages this document (see subsection 1.6.1). It remains in effect for the Certificates issued as per this document, until the end of life of the last Certificate issued in accordance with this CP/CPS.

9.10.2 Early expiry

This CP/CPS remains in force until it is replaced by a new version.

9.10.3 Effects of expiry - Clauses that remain applicable

Despite the replacement of this CP/CPS by a new version, the last Certificates issued when it was still valid entail the application of this document to said Certificates and to the various stakeholders until the Certificates in question expire.

9.11 Individual notification and communications between participants

The OTU PKI will inform its Subscribers via e-mail one (1) month at the latest before the publication of the new version of this document in the case of changes affecting this CP/CPS.

The Subscriber will also be informed of the effective implementation of the new version of the CP/CPS one (1) month at the latest after its publication via a signed e-mail announcement.
In addition, the Subscriber will be informed of any modification of the TS, GTOS or GTS through an e-mail announcement.

All the components and stakeholders of the OTU PKI are kept informed, through an internal announcement, of the changes made to this document and of the consequences that might result from these changes and which concern them.

This document does not impose any requirements with regard to the validation of changes by Subscribers. Indeed, the use of the services after the changes made have been notified is considered as full acceptance of these changes.

9.12 Amendments to the CP

9.12.1 Amendment procedures

The revisions of this CP/CPS are decided by the entity that manages the document, which is the Safety Committee (see subsection 1.6.1). Formatting changes (e.g. Spelling, etc.) or wording clarifications are not subjected to validation, and the CP can be updated without any prior notifications.

9.12.2 Amendment process and information period

In the event of a change requiring this CP/CPS to be modified, subsection 9.11 provides information about the procedure and information period applicable to amendments.

9.12.3 Circumstances under which the OID must be changed

If the Security Committee thinks that a change to the CP/CPS has consequences on the security or trust in the OTU PKI, it may define a new version of the Certification Policy, with a new OID.

9.13 Dispute resolution clause

The framework agreement signed between the Subscriber and Worldline or its duly authorized agent sets out the clauses with regard to dispute resolution. If there is no framework agreement, Worldline's GTS will be applicable.

The authorized contact for any comment, request for additional information, claim or submission of a litigation file concerning this CP/CPS is defined in subsection 1.6.2. All requests must be made via e-mail with acknowledgment of receipt or by registered mail with acknowledgment of receipt.

9.14 Jurisdiction

All of the OTU PKI's components including documentation are governed by the applicable legislation and regulations in force on the French territory even though some of the activities deriving from this CP/CPS might have legal effects outside of the French territory.

The framework agreement signed between the customer and Worldline, or its duly authorized agent, sets out this clause. If there is no framework agreement, Worldline's GTS will be applicable.

9.15 Compliance with laws and regulations

The OTU PKI is subjected to and applies the legislation and regulations in force on the French territory. Regular monitoring is performed to verify whether the PKI complies with these legal requirements.

Moreover, only the French version of the contractual documents listed in the GTOS (including this CP/CPS) is enforceable against the parties, even in the presence of translations. Indeed, translations, by express agreement, are provided for convenience only and have no legal effects, notably on the interpretation of the Subscription Contract or of the common intention of the parties.

9.16 Miscellaneous clauses

9.16.1 Global agreement

Not applicable

9.16.2 Activity transfers

Not applicable

9.16.3 Consequences of an invalid clause

Not applicable

9.16.4 Application and waiver

Not applicable

9.16.5 Force majeure

The concept of “force majeure” encompasses all the events that are usually recognized as such by French courts, notably irresistible, insurmountable, unpredictable events. Therefore, the OTU PKI may not be held liable for any indirect damage and interruption of its services due to force majeure.

The framework agreement signed between the customer and Worldline, or its duly authorized agent, sets out this clause. If there is no framework agreement, Worldline's GTS will be applicable.

9.17 Other clauses

9.17.1 Independence of the parties and non-discrimination

The roles within the OTU PKI that are in charge of generating Certificates and managing revocation are dedicated roles that are separate from the others functionally, technically, and hierarchically. These roles are fulfilled independently; therefore, they are not subjected to any commercial pressure that might be detrimental to the ethics and professional conduct of the trust services provided by the OTU PKI.

The issuance of Certificates at the Subscriber’s request, in accordance with this CP/CPS, does not make the OTU CA— including all the persons who make it up and represent it— agents or representatives of the Subscriber, Organization or Subject in any way whatsoever. The participants in this document do not constitute an association, a company or any other group.

The Organization set up as part of the OTU PKI, with effective role separation, makes it possible to preserve the impartiality of operations. In addition, the OTU PKI ensures that the trust activities provided are carried out equally for all beneficiaries.

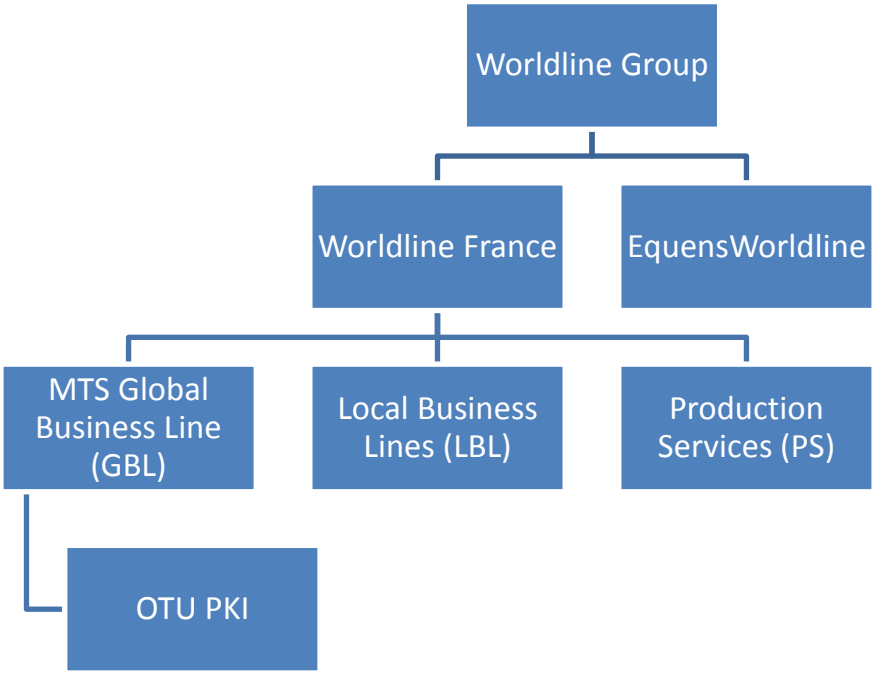

Figure 1 - Organizational diagram

The OTU PKI is centralized within the Global Business Line (GBL), which is a transverse unit of Worldline.
The Organization set up as by Worldline part of the OTU PKI, with effective role separation, makes it possible to preserve the impartiality of operations. (see Figure 1 - Organizational diagram)

9.17.2 Risk analysis

As part of the OTU PKI's activities, a Risk Analysis is carried out by the security manager of this PKI within their scope.

Its purpose is to identify ISS risks and the ISS measures implemented to deal with them. It ensures the consistency of the OTU CA's Information Security Policy with regard to the level of risk.

In particular, this document makes it possible to identify the obsolescence of algorithms, assets and their security needs applicable to the PKI's systems. It takes into account the state of the art in this area and is reviewed regularly by the OTU PKI's security officer. It is validated by the Security Committee following its review, which takes place every twenty-four (24) months at most.

9.17.3 Contractual Documents

In the event of a contradiction between the articles of the GTOS and those of the clauses of the higher-level service contract (framework agreement), the clauses of the GTOS, which derive from the applicable Certification Policy - Certification Practice Statement will prevail.

10 Appendices

REGULATIONS	
Reference	**Description**
[CNIL]	Law No. 78-17 of January 6, 1978 relating to data, files and freedom, amended by Law No. 2004-801 of August 6, 2004
[EIDAS]	REGULATION (EU) NO 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

TECHNICAL REGULATIONS	
Reference	**Description**
[RFC 3647]	Network Working Group – November 2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC 5280]	Network Working Group – May 2008 Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile
[RFC 6960]	IETF – June 2013 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP
[ETSI TS 119 312]	ETSI TS 119 312 v1.2.1 (2017-05) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	ETSI EN 319 401 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Certificates; Part 1: General requirements
[ETSI EN 319 412-2]	ETSI EN 319 412-2 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Certificates Profiles; Part 2: Certificate profile for Certificates issued to natural persons
[ETSI EN 319 412-3]	ETSI EN 319 412-3 v1.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Certificates Profiles; Part 3: Certificate profile for Certificates issued to legal persons

TECHNICAL DOCUMENTATION OF THE OTU PKI	
Reference	**Description**
[CPTD]	Certification Practice Technical Document OTU Certification Authority Reference: OTU DTPC 0003
[GTOS]	General Terms of Subscription to the OTU electronic signature and/or electronic Seal service OTU Certification Authority Reference: OTU CG 0008
[TS]	Terms of Service OTU Certification Authority Reference: OTU CG 0022
[ACP]	Activity Cessation Plan OTU Certification Authority Reference: OTU PCA 0027

[BCRP]	Business Continuity and Recovery Plan OTU Certification Authority Reference: OTU PCRA 0029
[VBOP]	Vendôme Backups Outsourcing Protocol Worldline Reference: Vendôme Backups Outsourcing Protocol
[IMP]	Incident Management Policy Worldline Reference: WLM-SEC-0008
[OSP]	OTU PKI's Operational Security Policy OTU Certification Authority Reference: OTU PSO 0015
[PDBHP]	Personal Data Breach Handling Procedure Worldline Reference: WLP-DPO-F017