**PUBLIC**

# ONLINE CAS CERTIFICATION POLICY - CERTIFICATION PRACTICES STATEMENTS

| | | |
|---|---|---|
| **AUTHOR(S)** | : | F. Da Silva |
| **DOCUMENT NO** | : | WLM-OTU-F002 |
| **VERSION** | : | 4.0 |
| **STATUS** | : | Final |
| **SOURCE** | : | Worldline |
| **DATE OF THE DOCUMENT** | : | April 23, 2019 |
| **NUMBER OF PAGES** | : | 93 |
| **DOCUMENT OWNER** | : | MediaCert Committee |

TSP MediaCert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2019-05-21 15:55:05

| Role | Name | Signature | Date |
|---|---|---|---|
| Reviewer 1 –Deputy Head of TSP | Fanny Lesecq | Fanny Lesecq | 23/04/2019 |
| Reviewer 2 - ISSM | Didier Sobkowiak | Didier Sobkowiak | 23/04/2019 |
| Quality insurance function | Fanny Lesecq | Fanny Lesecq | 23/04/2019 |
| Document owner | MediaCert Committee | Guillaume Bailleul | 23/04/2019 |
| Approver – Head of TSP | Guillaume Bailleul | Guillaume Bailleul | 23/04/2019 |

# Table of contents

# List of changes

| Version | Date | Description | Author(s) |
|---|---|---|---|
| 1.0 | 24/12/2012 | Initial public version | C. Brunet |
| 1.1 | 08/04/2013 | Evolution following remark during the initial audit ETSI 102 042 :<br>• 4.9.2.2.1: reformulation of the origins of the revocation<br>• 5.8.2: clarification on extended CRL in the event of cessation of activity | C. Brunet |
| 1.2 | 22/11/2013 | Evolution following contract adjustment:<br>• 3.2.3.3.1: additional explanations on the conservation of data not used in the Certificate<br>• 5.5.2: modification on the retention periods of registration files.<br>• 9.6.4: the term "immediately" shall be replaced by "as soon as possible".<br>• 9.9, 9.13, 9.14, 9.16.5: modification of the reference to Client/AWL contracts | C. Brunet |
| 1.3 | 01/02/2015 | Evolutions following change of company name and modification of the Certificate template:<br>• The whole document: Atos Worldline is replaced by Worldline (note that it is the same company with the same Siret)<br>• 7.1.2.2.3: modification in values indicated in the DN and Subject alt name and key usage fields | C. Brunet |
| 2.0 | 07/11/2016 | Developments following audit feedback<br>• Modification of §3.2.3.3.1 for Validation of the identity of a holder of a Single-use Certificate by external identification and, in the case of the holder belonging to the Subscriber's Organization, reformulation of the requirement to control the identity of the holder.<br>• Addition of procedures and reasons for destroying AC Key Twins in §6.3.4<br>• Change "operator" to "pilot".<br>• Homogenization of coverage limits with respect to the GCU (§9.7)<br>• Modification of §4.9.9.3.2 to describe the procedure for revoking an Organization Certificate<br>• Added methods to ensure that the revocation period is monitored (§4.9.3.2 and §5.7.3)<br>• Addition of §5.2.5 and §5.2.6 and amendment of §5.3.6 for CA compliance with the requirements of 7.4.3<br>• Addition of §5.4.6 on procedures for the restitution and control of the restitution of event logs<br>• Modification of §5.2.4 on roles requiring segregation of duties<br>• Adding OIDs to Test Certificates (§1.2.2.2) and adding descriptions (§7.1.2.4 and §7.1.2.5)<br>• Adding the oid of the PC OTU to the templates of all Certificates<br>• Addition of §4.9.10 on CRL archiving | V. Dumond<br>C. Lootvoet<br>A. Brugnot<br>J.J. Milhem |

| Version | Date | Description | Author(s) |
|---|---|---|---|
| | | • Added description of the monitoring of the Mediacert page (§2.4.2)<br>• Addition of a reference to the signature of CA documents to ensure authenticity control (§2.4.3)<br>• Revision of §5.3.2 on criminal record check<br>• Modification of templates and OIDs to track PC version change (§1.2.2.2, §7.1.2.2.2, §7.1.2.3, §7.1.2.3, §7.1.2.4, §7.1.2.5)<br>• Addition of a mention of the non-verification of the email when requesting a Certificate in §3.2.4<br>• Correction of § 7.1.5 Constraints on names that affect the CN attribute and also GN and SN if applicable for Organization Certificates<br>• Modification of §9.12.2 on the circumstances under which the OID must be changed<br>• Adding missing definitions<br>• Reformulations and clarifications concerning the contract, the subscription file, the subscriber's obligations, the identification of the Holder, the validation of an Organization<br>• Adding a step of acceptance of the Certificate by the OTU Certificate Holder<br>• Addition of non-discriminatory practical commitment to §9.6 | |
| 2.1 | 02/02/2017 | • Modification of the holder's information to be collected, verified and stored by the CA (§3.2.2.3.1)<br>• Review of CRL profiles (§7.2)<br>• Review of Certificate Templates (§7.1)<br>• Modification of the duration of the notice period in the event of a change in the CP (§9.11) | C. Lootvoet |
| 3.0 | 09/06/2017 | Rewriting to take into account eIDAS regulatory constraints | F. Lesecq<br>V. Dumond |
| 3.1 | 21/07/2017 | Taking into account the remarks of the eIDAS audit | F. Lesecq<br>F. Da Silva |
| 3.2 | 18/09/2018 | Integration of the document into the documentary structure of the MediaCert TSP, i.e. consistency with the GP<br>Adding causes for revocations in line with the update of ETSI EN 319 411-1 (v1.2.2)<br>Removal of the obligation to publish online<br>• older versions of CP-CPS<br>• English versions of the policies<br>Addition of a specification related to the DGMP and the retention of the identification information of an individual holding an OTU Certificate<br><br>Exceptionally, this version will not be published because it does not introduce new elements and a new version (with integration of a new CA in this document) will be published within the same time frame (more information in the safety meeting validation report) | F. Da Silva |
| 3.3 | 18/09/2018 | Addition of a CA to the scope of this document. The impact being only the addition of two ranges and the specification of the level of identification associated with them.<br>This CP-CPS then becomes the CP-CPS of the "online | F. Da Silva<br>V. Dumond |

| Version | Date | Description | Author(s) |
|---|---|---|---|
| | | CAs".<br><br>Taking into account the remarks/deviations detected during the 2018 surveillance audit of the OTU CA.<br><br>Review for consistency with the GDPR. | |
| 3.4 | 12/10/2018 | Consideration of the remarks/deviations detected during the 2018 certification audit of the OTU LCP CA:<br>• change of the description of the content of a CRL<br>• clarification of the list of means of validating consents<br>• review of the revocation conditions of OTU Certificates | F. Da Silva |
| 3.5 | 23/04/2019 | Review of the conditions for revocation of Single-Use Certificates (extension of the amendment made in v3.4)<br>Modification of the content's description of a CRL (cancels the modification made in v3.4)<br>Deletion of the reference to section 40 (human rights)<br>Evolution of standards versions in the repository | F. Da Silva |
| 4.0 | 23/04/2019 | New structure: under the DRP, the AC OTU is divided into two ACs (AC OTU & AC ORG) | F. Da Silva<br>J. Steux |

# 1 Introduction

## 1.1 General presentation

The MediaCert *Trust Service Provider*, established by Worldline, provides a set of Trust Services and is therefore subject to the eIDAS Regulation No 910/2014 of the European Parliament and of the European Council on electronic identification and trust services for electronic transactions in the internal market.

This document describes the Certification Policy of several Certification Authorities so-called "online", not qualified, operated by MediaCert TSP to govern the entire life cycle (creation, use, etc.) of Single-use Signature Certificates (also called "*One Time Usage*") implemented in the context of online subscription, but also of Electronic Stamp Certificates used to seal electronic data to guarantee their origin and integrity:

- the Certification Authority called "OTU LCP CA";
- the Certification Authority called "OTU CA".
- the Certification Authority called "ORG CA".

These CAs are operated in exactly the same way (organizational, technical, infrastructure, etc.), have the same hardware and software. However, they differ on different subjects:

| Subject of differentiation | OTU CA | ORG CA | OTU LCP CA |
|---|---|---|---|
| Use of the key pair / Certificate | Electronic signature certificate (see Chapter 1.5.1.1) | Electronic sealing certificate (see Chapter 1.5.1.1) | Electronic signature certificate (see Chapter 1.5.1.1) |
| Identification of the future holder of the Single-Use Certificate | requires a stricter level of identification for the provision of Single-Use Certificates than that defined by the LCP level but less strict than that defined by the NCP level, hence its so-called "enhanced" range (see Chapter 1.2.1); | X | requires a level of identification for the provision of single-use certificates in accordance with the LCP level, hence its so-called "standard" range (see chapter 1.2.1). |

This document presents in this context:

- the requirements to which each of these online CAs operated by MediaCert TSP are subject;
- the uses for which the Certificates are issued;
- the management of these Certificates in their life cycle;
- security measures around the Key Management Infrastructure also called Public Key Infrastructure;

- obligations and requirements relating to the different actors.

In addition to describing the Certification Policy, this document describes the Certification Practices Statements. This is the statement of practices that online Certification Authorities use in the management of the Certificates they issue.

In addition, as a Trusted Service provided by MediaCert TSP, all [GP] requirements and practices are, unless otherwise stated, applicable to the scope of these online CAs.

## 1.2 Identification

### 1.2.1 Document identification

| Elements | Value |
|---|---|
| Title | Online CAs Certification Policy - Certification Practices Statements |
| Document reference | WLM-OTU-F002 |
| OID | 1.2.250.1.111.20.5.4 |
| Version | 4.0 |
| Author | F. Da Silva |

The OID of this document is based on the OID "**1.2.250.1.111.20.5**": 1.2.250.1.111.20.20.5**.z.w** where:

- z: major version of this policy (e. g. version 3.1 → 3);
- w: type of Certificate used by online CAs.

As implied by the description above, online CAs have defined an OID for each of the types/ranges of Certificates they issue as follows:

| Scope | Certificate range | Compliance and targeted security level | OID |
|---|---|---|---|
| OTU CA | Single-use *"reinforced"* Certificates | [ETSI EN 319 411-1] LCP level *(not qualified)* | 1.2.250.1.111.20.5.4.1 |
| | Single-use "reinforced" test Certificates | [ETSI EN 319 411-1] LCP level *(not qualified)* | 1.2.250.1.111.20.5.4.3 |
| ORG CA | Organization Certificates | [ETSI EN 319 411-1] LCP level *(not qualified)* | 1.2.250.1.111.20.5.4.2 |
| | Test Organization Certificates | [ETSI EN 319 411-1] LCP level *(not qualified)* | 1.2.250.1.111.20.5.4.4 |
| OTU LCP CA | *"Standard"* Single-use Certificates | [ETSI EN 319 411-1] LCP level *(not qualified)* | 1.2.250.1.111.20.5.4.5 |
| | Single-use *"standard"* test Certificates | [ETSI EN 319 411-1] LCP level *(not qualified)* | 1.2.250.1.111.20.5.4.6 |

Further information is available in the General Policy [GP].

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

### 1.2.2 Identification of Certification Authorities

Unless otherwise specified, the requirements of this document are applicable to the CAs defined in chapter 1.1 this document. The requirements applicable to a single CA are preceded by the statement:

- [OTU LCP CA] for OTU LCP CA ;
- [OTU CA] for OTU CA;
- [ORG CA] for ORG CA.

These are linked to Worldline Root Certification Authorities whose necessary information is as follows:

| Scope | Elements | Value |
|---|---|---|
| OTU CA and ORG CA | CP-CPS *OID* | 1.2.250.1.111.20.3.1 |
| | Issuing CA OID | 1.2.250.1.111.20.3.1.3 |
| | Distinguish Name of root CA (DN) | C = FR<br>O = Worldline<br>OU = 0002 378901946<br>CN = MediaCert Trust CA - 2019 |
| OTU LCP CA | CP-CPS *OID* | 1.2.250.1.111.20.3.1 |
| | Issuing CA OID | 1.2.250.1.111.20.3.1.1 |
| | Distinguish Name (DN) of root CA | C = FR<br>O = Worldline<br>OU = 0002 378901946<br>CN = MediaCert Root CA 2018 |

The structure of the online CA Chains of Certification is as follows:

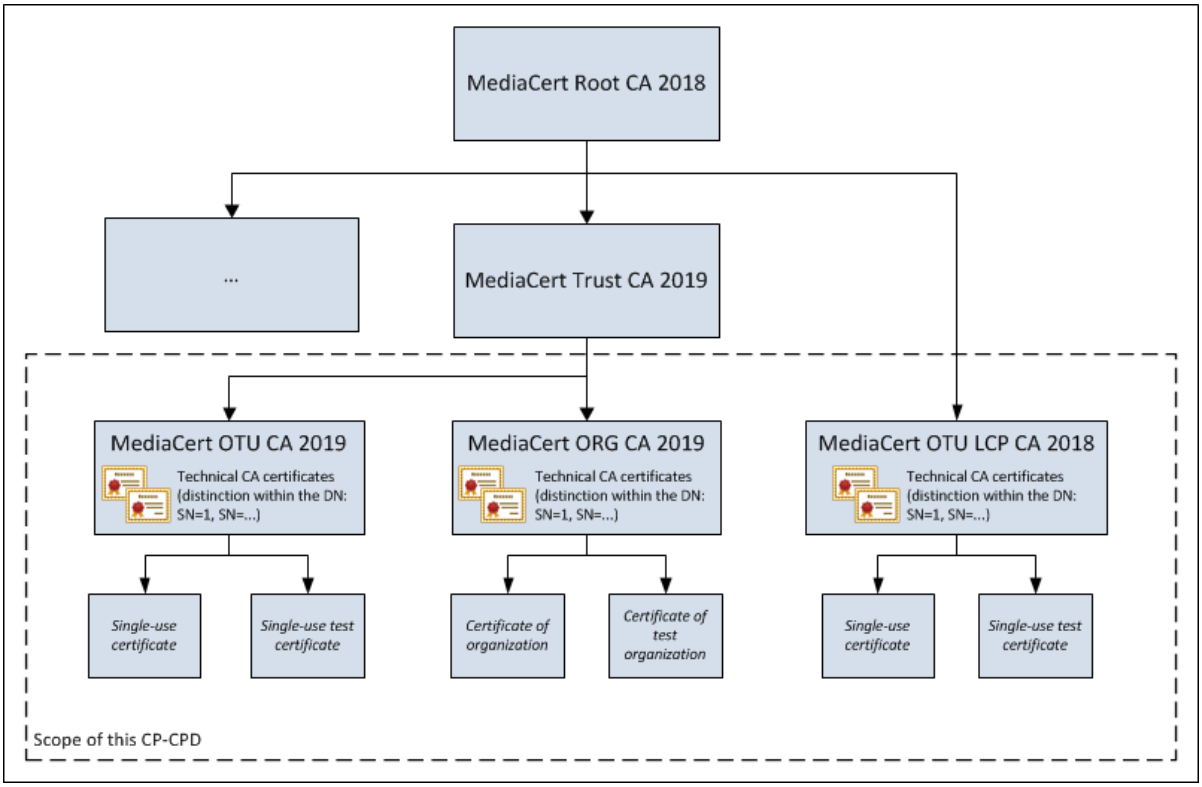


*Figure1 – OTU CA Chain of Certification*

## 1.3 Entities involved in Key Management Infrastructure

The Key Management Infrastructure consists of a set of dedicated technical, human, documentary and contractual resources to manage the life cycle of the electronic Certificates issued by the Certification Authority. It provides, through asymmetric cryptographic systems, a secure environment for electronic exchanges.

CAs rely on this technical infrastructure. The PKI's services are the result of different services that correspond to the different stages of the life cycle of Key pairs and Certificates. For this purpose, the PKIs concerned are made up of a number of entities as shown in the block diagram in figure 2.

The functional breakdown of the PKIs concerned by this CP-CPS is as follows:

- Registration service;
- Certificate generation service ;
- Certificate delivery service;
- Certificate revocation service;
- Information service on the status of Certificates.

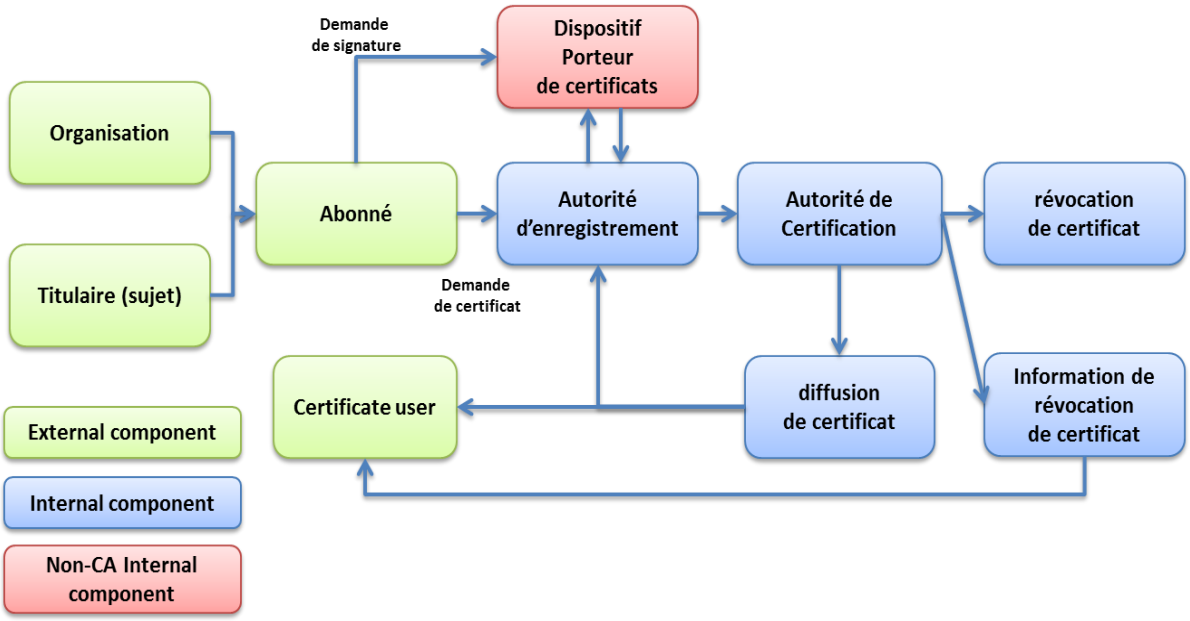


*Figure3 - Block diagram of PKIs operating online CAs*

### 1.3.1 Certification Authority

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

Online Certification Authorities are represented by a designated Authority Head within Worldline. This Authority Head is subordinate to Deputy Authority Heads, appointed by the Authority Head himself.

#### 1.3.1.1 Generation service

This service generates Certificates from:

- information transmitted by the Registration Authority; and
- of the public key of the Certificate from the secret element generation function.

These Certificates are electronically signed with the private key of the target CA and may only be used for the purposes described in chapter 1.5.1.1 of this document.

#### 1.3.1.2 Dissemination service

Once the Certificates have been generated, they are sent to the Registration Authority, which then forwards the Certificate to the Certificate Carrying Device.

#### 1.3.1.3 Revocation service

This service revokes Certificates based on a revocation request previously provided. The results are disseminated via the information services on the status of the Certificates.

#### 1.3.1.4 Certificate Status Information Service

This service provides Certificate users with information on the status of Certificates (revoked, suspended, etc.). This function is implemented through regularly updated publication modes: Revoked Certificate Lists (CRL), Revoked Authority List (ARL), and OCSP Responder.

### 1.3.2 Registration Authority

The Registration Authority is the interlocutor of the client units (Subscribers) that transmit requests to it to create or revoke Certificates. It therefore supports the following operations:

- authentication of the Subscriber who requests the creation of a Certificate;
- verification of the content of Certificate creation requests;
- [OTU CA][OTU LCP CA] verification of the correct application of the identification policy by Subscribers when issuing Single-use Certificates;
- [ORG CA] verification of the identity of the future Organization Certificate Holder;
- registration of requests to create and revoke Certificates;
- acceptance or refusal of requests to create and revoke Certificates;
- provision of Certificates to the Certificate Carrying Device;
- archiving of requests to create and revoke Certificates.

To provide these services, CAs operate their own Registration Authority (moreover, it is the same one) which relies on a service that has the technical and human resources to ensure the management of the life cycle of the Certificates they issue and which therefore constitutes a single access point to these Certification Authorities (servers allowing the transmission of applications and the delivery of Certificates).

### 1.3.3 Certificate Carrying Device

For the purpose of this CP-CPS, the Certificate Carrier Device is not considered to be the Certificate Holder.

Indeed, the Certificate Carrier Device refers here to a software and hardware entity hosted by Worldline that stores the Certificate and the private key of the Holder or an Organization.

For each Certificate generated by CAs, the Certificate Carrying Device is responsible for the following functions:

- generation of the Key pair;
- secure storage of the Key pair;
- generation of the Certification Request (CSR), containing the user information previously transmitted by the Subscriber;

- use of the private key and the Certificate in the cases of use described in chapter 1.5
- destruction of the private key as described in chapter 6.2.10.2 this document;

The Certificate Carrier Device provides secure storage and exclusive control on behalf of the Holder or Organization of the secret elements.

Exclusive control over Certificates is ensured:

- by the security features of the cryptographic box (protection of stored secrets);
- by a network isolation preventing any unauthorized server from connecting to these boxes.

The Certificate carrying device can have two (2) types of Certificates:

- Single-use Certificate: see chapter 1.4.1;
- Certificate of Organization: see chapter 1.4.2.

### 1.3.4 Certificate beneficiary

The provision of Certificates by CAs online requires the prior subscription to the services of these Certification Authorities. This requires the signature of a Subscription Contract with MediaCert TSP. This contract specifies the type of Certificate that the Subscriber wishes to implement:

- [OTU CA][OTU LCP CA] *One Time Usage* signature Certificate issued in the name of a natural person (Holder) in order to be able to sign Documents (see chapter 1.5.1.1); and/or
- [ORG CA] Certificate of Organization issued in the name of an Organization in order to be able to seal Documents in the name of its Organization or of its principal Organization (see chapter 11.5.1.1).

#### 1.3.4.1 [OTU CA][OTU LCP CA] Electronic signature service

If it is a question of signing electronic data, the two (2) online CAs then produce Single-use Certificates (see chapter 1.4.1).
In the case of Single-use Certificates, the Subscriber requests the creation of a Certificate from the Registration Authority by means of a technical process described in chapter 3.2.5.1. The Subscriber, in this case:

- must be identified to the Registration Authority (see chapter 3.2.2.1);
- must have identified it in such a way that the issued Certificate can be based on a reliable and verified identity (see chapter 3.2.3.1);
- must have obtained from the Holder the necessary consents to make a request to the RA to request the generation of a Single-use Certificate (see chapter 3.2.3.1).

#### 1.3.4.2 [ORG CA] Electronic sealing service

If it is a question of sealing electronic data on behalf of Organizations attached to the Subscriber, legally or by convention, the CA then produces Organization Certificates (see chapter 1.4.2).

Indeed, the Organization, via the Subscriber, will then use a Certificate operated by Worldline, to guarantee the integrity of the documents and authenticate their origin.

A Certificate of Organization may refer to the person who represents it legally, statutorily or by agreement. Either:

- the legal representative listed in the KBIS extract of the Organization;
- a person duly authorized, whether by agreement or by statute, to represent the Organization and to appear on the Certificate.

In all cases, the designated person must be duly authorized by the competent bodies within the Organization in order to be included on the Certificate.

The person who has the right to include his identity in the Certificate must provide proof of this to the Registration Authority in order to act as a representative of the Organization. If the Organization is not the Subscriber and it authorizes the Subscriber to act on its behalf, the Subscriber must justify to the Registration Authority his rights to act in the name of this Organization as well as the rights of the person designated to include his identity in the Certificate to represent the Organization.

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

A representative of the Subscriber must therefore be appointed in writing to the Registration Authority. This representative of the Subscriber may be:

- the Subscriber's legal representative (as it appears on a KBIS extract from the Subscriber less than three (3) months old);
- its conventional representative (as it appears, for example, on the articles of association);
- a representative authorized by the legal representative to represent the Subscriber in the performance of the Subscription Agreement.

Although the Subscriber and the Organization are in most cases one and the same entity, it is possible to differentiate them. For example, a Subscriber may wish to use a brand name rather than the name of the subscribing company. In addition, in the case of multiple subsidiaries of a group, the Subscriber and the Organization may not have the same name.

In all cases, the Subscriber must demonstrate the right he holds (ownership of the name, KBIS document, mandate, etc.) to indicate a name of Organization different from his own.

The Subscriber, via his legal or statutory representative, may formally designate in writing one or more deputy representatives of the Subscriber who are also authorized to represent him. To do so, it must inform the Registration Authority and grant them the necessary powers.

### 1.3.5 Certificate Users

The user of a Certificate is the natural or legal person who uses the information in a Certificate that he receives for the purposes described in chapter 1.5.1.1.

It is the responsibility of the users to verify the validity of the Certificate, at least before use, by using:

- the information contained in the Certificate (validity date, etc.);

- additional information provided by the CA such as the revocation status of the Certificate (see chapter 4.10).

It should be noted that the signature of a Document is mainly used by the products provided by the company ADOBE™, such as Acrobat Reader©. These products have document signature visualization functions.

Not all other Document Viewing products have signature viewer functions.

### 1.3.6 Other participants

Human resources complete the system:

- computer system operators (maintenance in operational condition);
- teams in charge of maintaining compliance.

## 1.4 Certificate Categories

Online CAs issue a number of Certificates:

- [OTU LCP CA] the CA produces two (2) types of Certificates;
- [OTU CA] the CA produces two (2) types of Certificates.
- [ORG CA] the CA produce two (2) certificates types

Each type of Certificate is distinguished by its OID (see chapter 1.2.1).

### 1.4.1 [OTU CA][OTU LCP CA] Single-use Certificates

A Single-use Certificate is dynamically produced by the Certification Authorities during the electronic signature process initiated by the Subscriber at the request of a natural person (Holder).

This Holder may be a natural person acting for its own needs or for the needs of its Organization and for which it is duly authorized to sign.

This Certificate is used during a single signature session (signature of the various Documents of a contract for the Holder) by the Certificate Carrier Device. It has a very short lifetime as described in chapter 6.3.2.

The Subscriber transmits the request for a Single-use Certificate to the Registration Authority by means of a message signed electronically by the Subscriber. This message contains:

- the Holder's identification data;
- an electronic stamp to guarantee the integrity of the identification data, as well as the identity of the Subscriber.

Once the Subscriber's Single-use Certificate application has been controlled and validated by the Registration Authority, the Certificate is issued by the target CA that signs the Certificate containing the identity of the Holder appearing on the Certificate, verified by the Subscriber.

Indeed, the Subscriber is responsible for the identification data transmitted in the application to the Registration Authority and which allows the creation of a Certificate containing verified data of the Holder.

The Holder's private key is generated in a secure and dedicated equipment in accordance with the information given in chapter 6.2.1.1 this document.

Once the Single-use Certificate has been used for the Holder at the Subscriber's request, the corresponding private key is destroyed in the HSM as described in chapter 6.2.10.2 However, the Certificate remains accessible in the signed document.

### 1.4.2 [ORG CA] Organization Certificates

The Organization Certificate is issued at the Subscriber's request to Worldline, on behalf of the Organization(s) for which the Subscriber is authorized to request a Document Seal (in accordance with the use defined in chapter 1.5.1.1). This service is operated by Worldline on its own premises.

The request for this type of Certificate is made according to a procedure between an authorized representative of the Subscriber and a Worldline Registration Operator. The information to be provided for the application is detailed in chapter 4.1.2.2 this document.

This CP-CPS does not make any face-to-face requirements but reserves the right to carry out additional checks of the counter-call type.

The private key of an Organization is generated in a secure and dedicated equipment in accordance with the information given in chapter 6.2.1.1.

### 1.4.3 Test Certificates

For technical purposes (test of presence and operation of the service), demonstration and acceptance of modifications made to the production information system, it is permitted to issue Test Certificates under the production CAs.

The Subscriber may indeed issue a request to create a Test Certificate to the Registration Authority, for his own use or for a Holder.

Under no circumstances may Test Certificates be used to bind the Holder, Subscriber or Worldline as a Production Certificate. However, the obligations of protection and use of the Certificate for the Holder, Subscriber and CAs are identical to those defined for Production Certificates.

For these Test Certificates, the attribute "*CommonName*" in the "*Subject*" field must be prefixed by the value "TEST" (see chapters 7.1.8, 7.1.9 and 7.1.10). These Certificates must be revoked as soon as their use is no longer necessary.

The limitations of use and liability applicable to Production Certificates also apply to Test Certificates.

## 1.5 Use of Certificates

### 1.5.1 Applicable fields of application

#### 1.5.1.1 Key pairs and Certificates holder

This CP-CPS deals with the Key pairs and electronic Certificates associated with these Key pairs, managed by the Certificate Carrying Device (defined in chapter 1.3.3 above), so that the Holders of electronic Certificates can, as part of the subscription or dematerialized transmission procedure:

- [OTU CA][OTU LCP CA] electronically sign a Document with a Single-use Certificate;
- [ORG CA] electronically seal a Document with an Organization Certificate.

#### 1.5.1.2 Key pairs and Certificates of CA and components

CA Key-Two are used exclusively to sign Certificates and CRLs whose templates are defined in chapter 7 of this document.
Their Certificate is signed by the Higher Level Certification Authority as described in chapter1.2.2 this document.

### 1.5.2 Prohibited areas of use

Any use other than that defined in the previous paragraph is prohibited by this CP-CPS. In addition, the Certificate must be used within the limits of the laws and regulations in force (see chapter 9.15.
MediaCert TSP cannot be held responsible for any misuse as specified.

## 1.6 CP management

### 1.6.1 Entity managing the CP

The entity managing this policy is indicated in the [GP].

### 1.6.2 Point of contact

The contact point is indicated in the [GP].

### 1.6.3 Entity determining the conformity of a CPS with this CP

This entity is described in the [GP].

### 1.6.4 Procedure for approving CPS compliance

The procedure for approving this CP-CPS is described in [GP].

## 1.7 Definitions and acronyms

### 1.7.1 Main definitions

A list of the main definitions of the technical terms used in this CP-CPS is provided below.

**Subscriber:** entity signing the Subscription Contract with the MediaCert TSP for delivery by online CAs:

- [ORG CA] of Organization Certificates at the request of duly authorized persons within the Subscriber who are legally and/or conventionally attached to it;

- [OTU CA][OTU LCP CA] Single-use Certificates in the name of the Holders as defined in this CP-CPS that the Subscriber has previously identified or that have been identified under his responsibility by duly authorized persons who are conventionally attached to him.

The Subscriber is in direct contact with the RA and performs a number of verifications for it, in particular concerning the identity and possibly the attributes of the Certificate User Holders.
In the case of Single-use Certificates, the Subscriber is mandated by the Holders to make an application on their behalf for Certificates.

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

**Certification Authority (CA):** the authority responsible for the application of this CP-CPS. Also refers to the technical entity that produces the Certificates at the request of the Registration Service and more generally manages them (manufacture, delivery, revocation, publication, logging, archiving) in accordance with this CP-CPS. For more information, see chapter 11.3.1.

**Technical Certification Authority (TCA):** Certification Authority acting under the name of the OTU Certification Authority,the ORG Certificate Authority or the OTU LCP Certification Authority.

**Registration Authority (RA):** authority in charge of receiving Subscriber Certificate requests, verifying these requests, archiving these requests and forwarding them to the Certification Authority. The term also refers to the technical entity in charge of implementing the Registration Service. For more information, see chapter 1.3.2.

**Key pair:** pair composed of a private key (to be kept secret) and a public key, necessary for the implementation of a cryptography service based on asymmetric algorithms (RSA for example).

**Electronic stamp:** data in electronic form, which are attached or logically associated with other data in electronic form to ensure the origin and integrity of the latter. This is also referred to as the "Organization Certificate".

**Certificate:** X509 standard data element used to associate a public key with its holder. A Certificate contains data such as the identity of the holder, his public key, the identity of the organization that issued the Certificate, the validity period, a serial number, a fingerprint *(digest*) or the criteria for use. This is signed by the private key of the CA that issued the Certificate.

**Daughter CA Certificate:** category of Certificates issued by Root CA to sign Daughter CA Certificates and Daughter CA Revocation Lists.

**ORG Certificate:** or Organization Certificate or Electronic Stamp; see chapter 1.4.2.

**OTU (One Time Usage) Certificate:** or Single-use Certificate; see chapter 1.4.1.

**Bearer Certificate:** category of Certificates issued by a daughter CA to Holders or Organizations. The Single-use Certificate and the Organization Certificate are Bearer Certificates.

**Chain of Certification:** all the Certificates required for the validation of the filiation of a Certificate issued to an entity.

**PKI component:** hardware platforms (computers, HSM, smart card reader) and software products playing a specific role within the PKI.

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

**Certification Practice Statement (CPS):** identifies the practices (organization, operational procedures, technical and human resources) that the CA applies in providing its Electronic Certification services to users and in accordance with the Certification policy(ies) to which it has committed itself.

**Certificate Request:** request made by the Subscriber to the Registration Authority to obtain a Certificate for a natural or legal person related to the Subscriber. This natural or legal person is identified and authenticated in advance by the Subscriber or by the persons duly authorized for this purpose under the responsibility of the latter. It includes a set of information to be provided by the Subscriber to the Registration Service with the Certificate application.

**Certificate Carrier Device:** a software component that obtains a Certificate(s) from the CA. These Certificates are used according to the applications and types of Certificates for uses defined in chapter 1.5.1.
The Certificate Carrier Device is composed of servers and cryptographic boxes operated jointly with the CA. It guarantees the exclusive control of the Key Twins and Certificates to the bearers.

**Document:** electronic static document in PDF format.

**Electronic registration file:** data container in electronic format, it is intended to contain all the data transmitted by a Subscriber during a Certificate creation request (information for the Certificate, Holder identification data, etc.). This data is archived in a probationary archiving system, which can be consulted at any time by the CA.

**Certificate Template:** computer data resulting from the registration deed of a Subscriber requesting a Certificate from the Registration Authority and which is then transmitted to the Certification Authority for signature.

**Hash or digital fingerprint:** refers to the result of a calculation function performed on digital content in such a way that even a slight change in the content results in the modification of the fingerprint. Hash is used to identify data and verify data integrity over time.

**Electronic identification:** the process of using personal identification data in electronic form that uniquely represents a natural person, a legal person or a natural person representing a legal person.

**Lightweight Certificate Policy (LCP):** Certification policy defined by [ETSI EN 319 411-1] offering a less expensive quality of service than the NCP (requiring less stringent policy requirements) to be used when a risk assessment does not justify the additional burden of meeting all NCP requirements (e.g. face-to-face identification).

**Normalized Certificate Policy (NCP):** Certification policy defined by [ETSI EN 319 411-1] which meets the best practices generally recognized by TSPs issuing Certificates.

**Organization:** entity representing in particular a company, a public administration, etc. or which may refer to a brand or company name for which an Organization Certificate or Electronic Stamp will be issued at the request of a Subscriber.

**Electronic identification means:** tangible and/or intangible element containing personal identification data and used to authenticate for an online service.

**Stakeholder:** in the context of this CP-CPS, the stakeholder is the entity that uses the Certificate it receives (here through an electronic signature. This signature is associated with a Document).

**PDF**: format of a computer file created by ADOBE Systems® and whose specificity is to preserve the formatting defined by its author.

**Certification Policy (CP):** published document describing all the rules and requirements with which the CA complies in the establishment and provision of trusted services. In particular, it indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. It also identifies the obligations and requirements relating to the various actors, as well as those weighing on all the components involved in the management of the Certificate life cycle.
The Certification policy is identified by an OID.

**Registration service:** see Registration Authority.

**Revocation management service:** see chapter 1.3.1.3.

**Information service on the status of Certificates**: see chapter 1.3.1.4.

**Signing session:** operation between the signing request and the return of the document(s) signed by the natural or legal person designated in the request. Several successive signatures can be made with the same Certificate in a Signing Session.

**Signatory:** a natural person identified in one or more electronic documents and who creates an electronic signature for that or those documents.

**Electronic signature:** according to the European eIDAS Regulation, these are data in electronic form, which are attached or logically associated with other data in electronic form and which the Signatory uses to sign.
According to the French Civil Code, a signature is used to identify the person who affixes it, to express his consent and to guarantee the integrity of the document to which he is attached.

It is recalled that the electronic signature implemented in this CP-CPS does not meet the definition of a qualified signature. According to the European eIDAS Regulation, the legal effect and admissibility of an electronic signature as evidence in court cannot be refused solely on the grounds that it is in electronic form or that it does not meet the requirements of a qualified electronic signature.

**Holder:** a natural person identified in the Certificate as the holder of this Certificate. The generation and exclusive use of the private key associated with the public key specified in the Certificate is entrusted to the Certificate Carrier Device.

**User**: see Stakeholder Part.

### 1.7.2 Acronyms

The acronyms used in this CP-CPS are as follows:

- **CA:** Certification Authority;
- **OTU CA:** Certification Authority issuing the Certificates described in this CP-CPS;
- **OTU LCP CA:** Certification Authority issuing the Certificates described in this CP-CPS;
- **RCA:** Root Certification Authority;
- **RA:** Registration Authority;
- **TSA:** Time-Stamping Authority;
- **CC:** Common Criteria;
- **CN:** Common Name;
- **CSR:** Certificate Signing Request;
- **DN:** Distinguished Name;
- **CPS:** Certification Practices Statement;
- **ETSI:** European Telecommunications Standards Institute;

- **HSM:** Hardware Security Module;
- **KC:** Key Ceremony;
- **PKI:** Public Key Infrastructure;
- **LAR:** List of Revoked Certification Authority Certificates;
- **CRL:** Certificates Revoked List;
- **OCSP:** Online Certificate Status Protocol;
- **RO**: Registration Operator;
- **OID:** Object Identifier;
- **CP:** Certification Policy ;
- **ISP:** Information Security Policy;
- **ISSM:** Information Systems Security Manager ;
- **RFC:** Request For Comment;
- **RSA:** Rivest Shamir Adelman;
- **SHA:** Secure Hash Algorithm;
- **URL:** Uniform Resource Locator;
- **UTC:** Universal Time Coordinated.

## 1.7.3 References

### 1.7.3.1 Regulation

| Reference | Description |
|---|---|
| [CNIL] | Law n°78-17 of 6 January 1978 relating to data processing, files and freedoms, as amended |
| [EIDAS] | REGULATION (EU) No 910 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing Directive 1999/93/EC |
| [GDPR] | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data |

### 1.7.3.2 Technical regulations

| Reference | Description |
|---|---|
| [RFC 3647] | Network Working Group - November 2003<br>Internet X.509 Public Key Infrastructure<br>Certificate Policy and Certification Practices Framework |
| [RFC 5280] | Network Working Group – May 2008<br>Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile |
| [RFC 6960] | IETF - June 2013<br>Internet X.509 Public Key Infrastructure<br>Online Certificate Status Protocol - OCSP |
| [ETSI TS 119 312] | ETSI TS 119 312 v1.2. 2 (2018-09)Electronic Signature and Infrastructures (ESI);<br>Cryptographic Suites |
| [ETSI IN 319 401] | ETSI EN 319 401 v2.2.1 (2018-04)<br>Electronic Signature and Infrastructures (ESI);<br>General Policy Requirements for Trust Service Providers |
| [ETSI IN 319 411-1] | ETSI EN 319 411-1 v1.2.2 (2018-04)<br>Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Certificates; |

| Reference | Description |
|---|---|
| | Part 1: General requirements |
| [ETSI IN 319 412-2] | ETSI EN 319 412-2 v2.1.1 (2016-02)<br>Electronic Signature and Infrastructures (ESI); Certificates Profiles;<br>Part 2: Certificate profile for Certificates issued to natural persons |
| [ETSI IN 319 412-3] | ETSI EN 319 412-3 v1.1.1 (2016-02)<br>Electronic Signature and Infrastructures (ESI); Certificates Profiles;<br>Part 3: Certificate profile for Certificates issued to legal persons |

#### 1.7.3.3 Internal documentation

| Reference | Description |
|---|---|
| [TDCP] | Technical Documentation of Certification Practices<br>Online Certification Authorities<br>Reference: WLS-OTU-F003 |
| [GCSubscription] | General Terms and Conditions of Subscription to the OTU electronic signature service and/or electronic stamp<br>Online Certification Authorities<br>Reference: WLS-OTU-F008 |
| [GCServices] | General Terms and Conditions of Services<br>Online Certification Authorities<br>Reference: WLS-OTU-F022 |
| [BCP] | Business Closure Plan<br>Online Certification Authorities<br>Reference: WLS-OTU-F028 |
| [CBRP] | Continuity and Business Resumption Plan<br>Online Certification Authorities<br>Reference: WLS-OTU-F029 |
| [VBOP] | Vendôme Backup Outsourcing Protocol<br>Worldline<br>Reference: Vendôme Backup Outsourcing Protocol |
| [GP] | General Policy of the MediaCert TSP<br>MediaCert TSP<br>Reference: WLM-TSP-F094<br>OID: 1.2.250.1.111.20.1.1 |
| [IMP] | Incident Management Policy<br>Worldline<br>Reference: WLM-SEC-0008 |
| [PHPDV] | Procedure for Handling Personal Data Violations<br>Worldline<br>Reference: WLP-DPO-E017 |

#### 1.7.3.4 External documentation

| Reference | Description |
|---|---|
| [ANSSI Notification] | National Agency for Information Systems Security (ANSSI)<br>Form for reporting a security incident related to a qualified product or service |

# 2 Responsibilities for the provision of information to be published

## 2.1 Entities responsible for making information available

The entity described in the [GP] document in the corresponding chapter is the entity responsible for making available the information to be published described in chapter 2.2 this document. The publication site is described in the [GP].

## 2.2 Information to be published

The information published by the CAs online on the MediaCert TSP website is as follows:

- this CP-CPS;
- the current General Terms and Conditions of Services [GCServices];
- the current general terms and conditions of subscription [GCSubscription];
- the current general terms and conditions of sale (GCSales);
- lists of revoked Certificates (CRL);
- the valid online CA Certificate;
- Certificates of the test range.

This CP-CPS is published in PDF/A format.

The URLs for accessing this CP-CPS as well as the LCR and OCSP answering machine are available in the extensions of Certificates issued by CAs in accordance with chapter 7.1 this document.

The Evidence Management Policy is made available to the Subscriber upon electronic request (via e-mail) at the contact point defined in chapter 1.6.2 of this document.

## 2.3 Publication deadlines and frequencies

All requirements and practices described in the [GP] in the corresponding chapter apply.

In addition, certification policies are regularly updated and published, particularly in the event of major changes (see chapters 9.11 and 9.12).

The time frame and frequency of publication of information on the status of the Certificates are indicated in chapters 4.9.8 and 4.9.7 this document respectively. In addition, CA Certificates are published following their generation and before any Certification.

## 2.4 Access control to published information

All requirements and practices described in the [GP] in the corresponding chapter apply.

# 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 each X509 compliant Certificate, the "*Issuer*" (issuing CA) and "*Subject*" fields are identified by a "*Distinguished Name*" (DN) of type X.501 in the form of a "*PrintableString*".

### 3.1.2 Need to use explicit names

#### 3.1.2.1 [OTU CA][OTU LCP CA] Single-use Certificates

In the case of Single-use Certificates, Certificates issued in the name of the Holder under this CP-CPS contain the first and last name appearing in the valid identity documents submitted by the Holder.

#### 3.1.2.2 [ORG CA] Organization Certificates

In the case of an Organization Certificate, the Certificates issued contain:

- the Subscriber's name; and
- the name of the Organization; and
- the first and last name appearing in the valid proof of identity presented by the person authorized by the Subscriber to represent this Organization; or
- the name of the unit in the Organization for which the Certificate is intended.

### 3.1.3 Anonymization or pseudonymization of the bearers

The Certificates covered by this CP-CPS may under no circumstances be anonymous. The names provided for the issuance of a Certificate may under no circumstances be pseudonyms.

### 3.1.4 Rules for the interpretation of different forms of names

The interpretation of information such as the "*Distinguish Name*" field is indicated in each Certificate template in chapter 7 this CP-CPS.

### 3.1.5 Uniqueness of names

The "*Distinguished Name*" (DN) is unique for each Holder or Organization. Any request from the Subscriber that does not comply with this rule is refused by the Registration Authority (see chapter 4.2.1). Throughout the life cycle of the CAs and after they cease to operate, a "*Distinguished Name*" (DN) assigned to a Holder or Organization by these CAs cannot therefore be assigned to another Holder or Organization.

The rules applied to obtain this uniqueness on DN are as follows:

- [OTU CA][OTU LCP CA] for Single-use Certificates, uniqueness is guaranteed by:
    - the identifier of the trace container in the "*Common Name*" field of the DN; and
    - the "*SERIALNUMBER*" field of the DN ;
- [ORG CA] for Organization Certificates, uniqueness is guaranteed by:
    - the "*Organization ID*" field of the DN which must be unique for each Organization. This is verified by the RA upon acceptance of the creation request; and
    - the "*SERIALNUMBER*" field of the DN.

More information on the construction of some of these fields is available in chapter 7.1 this document.

### 3.1.6 Identification, authentication and role of trademarks

The information is available in chapter 3.2.2.2 this CP-CPS.

## 3.2 Initial identity validation

### 3.2.1 Method for proving possession of the private key

#### 3.2.1.1 [OTU CA][OTU LCP CA] Single-use Certificates

In the case of short-term use (see chapter 6.3.2), the possession control of the private key is performed by means of a low-level cryptographic verification of a first signature produced by means of the private key.

If the verification fails, then:

- the Document is not signed;
- the private key is destroyed (see chapter 6.2.10.2);
- the Subscriber who made the request receives an error message informing him/her of the failure of the request.

The Certificate Holder is not subject to this proof of possession.

#### 3.2.1.2 [ORG CA] Certificate of Organization

Proof of possession of the private key provided by the Certificate Carrier Device is guaranteed during the generation of the request by signing the message with the private key that corresponds to the public key contained in the PKCS#10 (CSR) message sent to the Registrar Authority.

These query formats include a signature by the corresponding private key to ensure the integrity and proof of possession of the private key.

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

## 3.2.2 Validation of the identity of organizations

### 3.2.2.1 Validation of a Subscriber

The validation of a Subscriber's identity requires following the steps described below and collecting all the required information. The Registration Authority keeps all the documents sent when the Subscriber subscribes to the Service.

#### Signing of the Subscription Contract

The status of Subscriber is subject to the prior establishment of a contractual relationship between the Subscriber and the MediaCert TSP. This is the Subscription Contract for the Single-use electronic signature service and/or Electronic Stamp. The signature of this Subscription Agreement certifies in particular the acceptance of the Subscriber's obligations described in this document in chapter 9.6.3.1 General Terms and Conditions of Subscription [GCSubscription] (documents attached to the Subscription Agreement).

#### Appointment or appointment of representatives within the Subscriber

A Subscriber's representative must then be appointed to the Registration Authority so that he/she can become the latter's contact person for requests for Organization Certificates. This representative of the Subscriber may be:

- the Subscriber's legal representative (as it appears on a KBIS extract from the Subscriber less than three months old);
- its conventional representative (as it appears, for example, on the articles of association);
- a representative authorized (delegation, power or mandate) by the legal representative to represent the Subscriber in the performance of the Subscription Contract.

The Subscriber, via his legal or statutory representative, may formally designate in writing (via the information sheet of the Subscriber's deputy representative to the online CAs provided by the Registration Authority) one or more deputy representatives of the Subscriber who are also authorized to represent him. To do so, it must inform the Registration Authority and grant them the necessary powers.

#### Provision of the necessary documentation when subscribing to the Subscriber Agreement

In addition, when signing the Subscription Contract, the designated Subscriber's representative must provide:

- the General Terms and Conditions of Subscription [GCSubscription] that it has initialed or had initialed by the Organization's legal representative;
- the information sheet of the Subscriber's representative to the online CAs, provided by the Registration Authority, duly completed and signed by the Subscriber's representative. This form contains, among other things, the Subscriber's physical address and a valid e-mail address of his representative, allowing him to be contacted. This e-mail address will be used, among other things, to transmit information when creating Organization Certificates; and
- the identification policy that it implements, in compliance with the prescriptions and recommendations made to it by the Registration Authority, only in the event that it wishes

to subscribe to the Single-use Certificate service. This must be validated by the RA and can be controlled by the RA as written in chapter 3.2.3.1; and

- a copy of an official identity document valid at the time of contractualization containing an identity photograph from among the documents defined below: national identity card, passport or residence permit; and

- a KBIS extract dating from less than three (3) months before the contractualization, or the published statutes in force of the Organization to which it belongs, including its name and capacity and any valid documents necessary to justify its powers;

- if it does not appear on the KBIS extract dating back less than three (3) months, or on the published statutes of this Organization in force, it must be duly authorized by the Subscriber's legal representative within the framework of a written power of attorney to represent him/her with the exhaustive nature of the powers granted to him/her.

All these elements are also mentioned in a notice that is provided to the Subscriber with the Subscription Contract.

### 3.2.2.2 [ORG CA] Validation of an Organization

The validation of an Organization as a beneficiary of the services is based on the prior validation of the Subscriber's identity (see chapter 3.2.2.1). It is done upon receipt of a request to create a Certificate, the CA's contact person being only the Subscriber.

As described in chapter 1.3.4.2, an Organization is represented by an authorized individual: the representative of the Organization. The information concerning the Organization to be sent to the Registration Authority by the Subscriber when requesting the creation of a Certificate is as follows:

***In the event that the Organization and the Subscriber are two different entities***

- any document, valid at the time of the Certificate creation request, demonstrating the Subscriber's right and authority to include the Organization's name in the Certificate.

***In all cases***

- if the General Terms and Conditions of Subscription [GCSubscription] have changed since the contract was concluded or the last request to create a Certificate, the said updated document must be returned initialed by the legal representative or by the representative of the authorized Subscriber;

- a request to create a Certificate, signed and dated by a legal representative, by the Subscriber's representative or one of his deputies, specifying :

    - the name of the Subscriber to be included on the electronic Certificate; and

    - the name of the Organization to be included on the electronic Certificate; and

    - the full name of the individual authorized to represent the Organization and identified in the Certificate; or

    - the name of the unit in the Organization for which the Certificate is intended.

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

- any document, valid at the time of the request for the creation of the Certificate, attesting to the existence of the Organization (extract from KBIS dated less than three (3) months ago or, original or copy of any official deed or extract from the official register dated less than three (3) months ago attesting to the name, legal form, registered office address and identity of the partners and corporate officers mentioned in 1° and 2° of Article R. 123-54 of the Commercial Code or their equivalents under foreign law,...);

- indeed, when the identity of an individual comes to be included in the Certificate, the Subscriber must transmit to the Registration Authority:

    - any document, valid at the time of the request to create a Certificate, to demonstrate the membership of the authorized individual in the Organization;

    - a copy of a valid official identity document of the authorized individual from the following documents:

        - national identity card;

        - passport ;

        - residence permit.

      The Registration Authority keeps this copy.

    - the postal address, an e-mail address and a telephone number allowing the Registration Authority to contact this authorized individual.

This CP-CPS does not set out any requirements for face-to-face identification. However, the Registration Authority may carry out additional verifications.

### 3.2.3 Validation of an individual's identity

#### 3.2.3.1 [OTU CA][OTU LCP CA] Single-use Certificate

The request to create a Certificate in the name of a Holder is made by the Subscriber to the Registration Authority.
This request is made in electronic form because it must be signed by the applicant by means of an electronic signature (see chapter 3.2.5.1). It contains at least the following Holder data:

- his first and last name;

- his date and place of birth.

The Subscriber can also specify for the registration file:

- the courtesy of the Holder;

- the Holder's mailing address;

- the telephone number of the Holder;

- the email address of the Holder.

The Subscriber may supplement the information provided above with information known in advance and specific to the future Holder, making it possible to identify it within a pre-established database.

Only the Holder's "first and last name" information is included in the Certificates produced by the CAs. However, all the above-mentioned information is kept by the Registration Authority in the registration file in electronic format associated with the issuance of the Certificate, in accordance with chapter 5.4 this document, in order to support the proof of identification.

The conservation of this data is necessary because it is provided for the constitution of the registration file which is associated with each issuance of a Certificate. This registration file gathers the data mentioned above, describing the processes and identification data of the final customer (Holder).

Chapter 3.1.5 this document also defines how the uniqueness of the "*Distinguished Name*" in Single-use Certificates is guaranteed.

***Identification policy***
The Subscriber must specify to the RA in writing, when contracting with the MediaCert TSP for the issuance of Single-use Certificates, the identification policy he has put in place (see chapter 33.2.2.1 section *"Provision of the necessary documentation at the time of subscription to the Subscriber Agreement*") in order to verify the civil identity declared by the future Holder.

The identification procedures contained in this policy must be based at least on the verification of a valid official document bearing a photograph of the Holder (national identity card, passport or residence permit) or on any other valid official procedure enabling or having enabled, prior to the issue of a Certificate, to verify the declared identity of a Holder. More specifically:

- [OTU LCP CA] the identity of the future Holder may be checked automatically in order to verify the declared identity of the Holder;

- [OTU CA] the identity checks of the future Holder must be carried out by operators in order to be able to verify the Holder's identity in a physical way.

In any case, during the identification process, checks on the identity of the future Holder must be based on legally valid identity documents, which may be presented in some countries in electronic form. Indeed, in some States, the identification step may be carried out on the basis of an electronic identity card or may rely on other legally valid electronic means of identification to achieve reliable identification. In this context, the Subscriber verifies that the Holder is indeed the holder of a valid electronic identity card or possesses other legally valid electronic means of identification to achieve reliable identification.

These identity documents in physical or electronic form are used to support the identification data that the Subscriber has previously collected from the Holder, with the issuance of a Single-use Certificate as part of the electronic signature process.

The particulars to be recorded, verified and kept include the person's first names, surnames, date and place of birth, as well as the nature and date of issue of the document.

The Registration Authority reserves the right to assess the reliability of the identification process put in place and not to issue a Certificate if the Subscriber's identification policy is assessed as not providing a sufficient level of reliability. In particular, RA will regularly monitor this policy by sampling in accordance with the RA sampling procedure. In the event of deviations from the said procedure, the Subscriber undertakes to establish an action plan with MediaCert TSP to resolve such deviations. Non-application of this action plan or the observation of discrepancies during the next sampling campaign may lead to the deactivation of the Electronic Signature service using Single-use Certificates.

The above-mentioned identification policy is supplemented by a description of the process that will be used by the Holder to consent to proceed with an electronic signature using the Single-use Certificate (Consent Collection Policy).
This consent collection policy details, for each of the consents to be obtained in the context of the implementation of this electronic signature, the identification of the means by which the Holder will express its agreement. Before being able to sign electronically, the Holder must, in fact:

- be aware of the conditions of use of the electronic signature and its obligations as described by the Subscriber in a durable medium made available to him in a readable and explicit form;
- consent to the signature, in electronic form, in the context of the transaction to which it is a party by accepting the terms and conditions relating to the use of the Single-use Certificate;
- accept the keeping of a register by the Registration Authority allowing it to process and keep the identity information used necessary for the generation of the Single-use Certificate, for the duration fixed by the exercise of its mission and the related audits;
- in the context of automated identity checks, give its consent to the automation of the said check;
- confirm the validity of the information contained in the Certificate;
- as a consequence of the above, give the Subscriber an express mandate to proceed to the Registration Authority with an application for a Single-use Certificate so that he can sign. It is specified that in this context, the consents given by the Holder initiate an automated request in the Subscriber's name for an electronic signature from the Registration Authority.

The validation procedures of the expression and the obtaining of the consent of the Holder chosen by the Subscriber may be one of the following:

- an electronic capture of the Holder's handwritten signature;
- sending an OTP code received by SMS to the Holder's personal mobile phone.

The above list is for illustrative purposes only and is not exhaustive.

As the identification process is described by the Subscriber, it is up to him/her to:

- implement it or have it implemented under its responsibility. If persons are designated and authorized by the Subscriber to perform this identification under his responsibility, this must then be stipulated by the Subscriber in the identification policy he provides to the Registration Authority;
- transmit to the RA, in an electronic registration file, the captured identification data and proof of identity provided to it during the implementation of the electronic signature process.

***Exceptions to the principle of transmission of elements justifying the identity of Holders to RA***
The Subscriber therefore transmits to the Registration Authority digital copies of all the elements used to verify the identity of the future Registrant, except in the following cases:

- the holder belongs to the Subscriber's Organization. Indeed, there is no need for the Subscriber to carry out an additional identity check if the Subscriber has provided the

future Holder with a reliable means of authentication accepted by the RA, in particular to access his professional mailbox or to connect to the application requiring the latter's signature.

In this context, the Subscriber must ask the future Holder to ensure the security of his computer, his professional mailbox and his identifiers.

The RA is required to ensure that the Holder was a member of the Subscriber's Organization at the time of signature by performing sample checks as mentioned above in this chapter.

- the Subscriber retains the identity verification elements of the future Identity Holder on behalf of RA. In this context, the Subscriber must keep these elements in a secure manner. The RA will then make the necessary declarations to the CNIL in order to be able to meet the obligations imposed on Certification Authorities towards their auditors.

  The RA is required to ensure that the verification of the identity of the future Holder has actually been implemented by the Subscriber by performing sample checks as mentioned above in this chapter.

#### 3.2.3.2 [OTU CA] Certificate of Organization

The information is available in chapter 3.2.2.2, section *"Concerning the Subscriber's right to include the name of the Organization in the Certificate".*

### 3.2.4 Unaudited information

Certificates issued by Certification Authorities pursuant to this CP-CPS do not contain any unverified information except for the e-mail and the *Organization Unit* (OU) field corresponding to the Organization's unit name within the *Subject*'s *Distinguished Name* (DN).

### 3.2.5 Validation of the applicant's authority

Whether it is a Single-use Certificate or an Organization Certificate, the request is made by the Subscriber, who must be identified before any request to create a Certificate is made, the initial validation of a Subscriber being described in chapter 3.2.2.1.

At the time of each request to create a Certificate, the Subscriber authenticates himself to the Registration Authority and the Certificate Carrying Device. Authentication is done differently depending on the type of Certificate requested.

#### 3.2.5.1 [OTU CA][OTU LCP CA] Single-use Certificates

When requesting the creation of a Single-use Certificate and signature from the Registration Authority (which then contacts the Certificate Carrying Device), the Subscriber must authenticate himself and sign the request electronically.

The Subscriber's authentication is then done by Certificate. This Certificate must be issued by a Certification Authority approved by the MediaCert TSP as described in the document [TDCP].

#### 3.2.5.2 [ORG CA] Certificate of Organization

When the Subscriber's representative requests the creation of a Certificate of Organization from the Registration Authority, the Subscriber's representative is authenticated by the Registration Authority.

The Subscriber's authentication is then done by a signed handwritten request. The authenticity of this request is verified by the RA using the signature on the copy of the proof of identity, kept by the RA, as well as a set of elements related to the commercial relationship that Worldline has with the Subscriber.

### 3.2.6 Interoperability criteria

This CP-CPS does not make any requirements in this regard.

## 3.3 Identification and validation of a key renewal request

### 3.3.1 [OTU CA][OTU LCP CA] Single-use Certificates

For the purpose of this CP-CPS, there is no key renewal function for this category of Certificate. Indeed, as the name suggests, this type of Certificate is for single use only.

#### 3.3.1.1 Identification and validation for a current renewal

Not applicable.

#### 3.3.1.2 Identification and validation for renewal after revocation

Not applicable.

### 3.3.2 [ORG CA] Organization Certificates

For this category of Certificate, a key renewal request is treated as an initial creation request. Therefore, a new Organization Certificate cannot be provided without renewal of the corresponding Key pair as well (see chapter 4.6).

#### 3.3.2.1 Identification and validation for a current renewal

Not applicable.

#### 3.3.2.2 Identification and validation for renewal after revocation

Not applicable.

## 3.4 Identification and validation of a revocation request

### 3.4.1 [OTU CA][OTU LCP CA] Single-use Certificate

When using a Certificate with such a short lifespan (see chapter 6.3.2), revocation can only occur when used during a Signing Session. Therefore, a Holder's Certificate can only be revoked at the request of the Certificate Carrying Device (see chapter 4.9.2.1).

This request is therefore transmitted by the Certificate Carrier Device to the Registration Authority, which then redirects the request to the Certificate Authority issuing the Certificate concerned by the revocation. The latter automatically validates the request and then carries out the revocation online.

Any request for revocation of a Single-use Certificate from the Certificate Carrier Device is considered valid.

### 3.4.2 [ORG CA] Certificate of Organization

An Organization Certificate may be revoked by:

- the person authorized and designated in the Certificate in question, or a person explicitly authorized and designated by him. The request is then forwarded to the Registration Authority, which redirects it to the Certification Authority for validation and execution if the request is in order;
- the Certification Authority issuing the Certificate.

Identification is then carried out as defined in chapter 4.9.3.2.

# 4 Operational requirements over the life cycle of Certificates

## 4.1 Request to create a Certificate

### 4.1.1 Origin of a request

#### 4.1.1.1 [OTU CA][OTU LCP CA] Single-use Certificates

The creation of a Single-use Certificate can only be requested by a Subscriber identified to the Registration Authority (see chapter 3.2.2.1). Before making any request to the RA, the Subscriber undertakes to identify the future Holder or to have it identified under his responsibility and to obtain the Holder's consent as described in chapter 3.2.3.1 that he can benefit from this service.

#### 4.1.1.2 [ORG CA] Organization Certificates

The creation of an Organization Certificate can only be requested by a Subscriber identified to the Registration Authority via his representative or deputy representative, in accordance with chapter 3.2.2.1.

### 4.1.2 Process and responsibilities for preparing an application

#### 4.1.2.1 [OTU CA][OTU LCP CA] Single-use Certificates

All the information that must be included as a minimum in the request is specified in chapter 3.2.3.1 this CP-CPS.

The request is established by the Subscriber on the basis of information collected from reliable sources and valid supporting documents from the Holder (see chapter 4.1.1.1).

The Subscriber undertakes to Worldline through the Subscription Agreement to:

- inform the Registration Authority, in writing, of its procedures for identifying the future Registrants it wishes to implement through the provision of its Identification Policy;
- implement the said procedures for identifying the future Holder, defined in its identification policy in accordance with chapter 3.2.3.1 and apply them before proceeding with any request to create a Certificate in the name of the future Holder;
- inform the future Holder of the various steps he will have to take in order to award a Certificate in his name in order to be able to sign electronically the document or documents presented to him by the Subscriber and, to this end, obtain the prior agreement of the future Holder to the choice of the electronic signature to sign these documents and the obligations resulting from this choice as specified in chapter 3.2.3.1 including the power to give the Subscriber the power to make requests for a Single-use Certificate for the benefit of the Holder to the Registration Authority and to accept the processing of his personal data by the RA and the CA;
- as a result of the above, inform the future Holder of the processing of his personal information by the RA and the CA and to this end obtain the necessary prior consents from him to the processing and storage of his data in the context of the generation of the Single-use Certificate and the management of evidence;
- provide all the information necessary for the issuance of the Certificate.

Once the application has been sent to the Registration Authority and validated, it is sent to the Certification Authority for the generation of the Single-use Certificate on behalf of the Holder.

MediaCert TSP cannot be held liable if the Subscriber and/or the Holder do not respect the commitments they have accepted to benefit from the electronic signature service.

MediaCert TSP reserves the right to refuse to issue a Single-use Certificate if it is found that the obligations of the Holder, related to the Subscriber, and/or the Subscriber's obligations are not respected.

#### 4.1.2.2 [ORG CA] Organization Certificates

All the information that must be included as a minimum in the request is specified in chapter 3.2.3.2 this CP-CPS.

The request is established by the Subscriber's representative through a request file for the creation of an Organization Certificate. This file is completed by the Organization's authorized representative and then sent to the Registration Authority, which processes the application as defined in chapter 4.2.1.2 this document.

MediaCert TSP cannot be held liable if the Subscriber does not respect the commitments it has accepted under the Subscription Contract.

MediaCert TSP reserves the right to refuse to issue an Organizational Certificate if it appears that the Subscriber's obligations are not respected.

## 4.2 Processing a request to create a Certificate

### 4.2.1 Execution of the identification and validation processes of the request

#### 4.2.1.1 [OTU CA][OTU LCP CA] Single-use Certificates

Once the Subscriber's request has been received by the Registration Authority, it carries out the following operations:

- verification of the Subscriber's identity (see chapter 3.2.2.1): the RA verifies the information transmitted by the Subscriber and verifies that the latter is actually known to him/her;
- request verification: RA verifies that the Subscriber's request is electronically signed on its behalf;
- validation of consents and Holder identity data: the RA validates the presence of the necessary information (see chapter 3.2.3.1). The signature of the request, made by the Subscriber, attests to the validity of the information provided for inclusion in the Certificate.

Once these operations have been performed, if everything is correct then the Registration Authority issues the Certificate generation request to the target CA and keeps a record of the Subscriber's request archived in digital format.

[OTU LCP CA] The CA will then generate a Certificate containing the holder's identity data as defined in chapter 7.1.4 this document.

[OTU CA] The CA will then generate a Certificate containing the holder's identity data as defined in chapter 7.1.6 this document.

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

#### 4.2.1.2 [ORG CA] Organization Certificates

Once the Subscriber's representative's request has been received by the Registration Authority, it carries out the following operations:

- validation of the identification data of the Organization and the individual representing it within the Organization (see chapter 3.2.2.2): completion, uniqueness and accuracy of the information;
- verification of the completeness of the application file for the creation of a Certificate of Organization: the RA ensures in particular that it has information enabling it to contact the future Certificate Holder.

Once these operations have been performed, if everything is correct then the Registration Authority issues the Certificate generation request to the OTU CA and keeps a record of the Subscriber's representative's request archived in digital format.

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

### 4.2.2 Acceptance or rejection of the request

#### 4.2.2.1 [OTU CA][OTU LCP CA] Single-use Certificates

Acceptance or rejection is done automatically.

In the event of rejection of the application, the Registration Authority shall inform the Subscriber by means of a technical notification at the Subscriber's request. The notification shall include the justification for the rejection. A new request must be made.

#### 4.2.2.2 [ORG CA] Organization Certificates

Acceptance or rejection is done manually.

In the event of rejection of the application, the Registration Authority shall inform the contact point identified in the application, justifying the rejection. The RA may then request missing documents to complete the registration file, but may in no case modify the signed data. A new request must be made.

### 4.2.3 Time limit for issuing the Certificate

#### 4.2.3.1 [OTU CA][OTU LCP CA] Single-use Certificates

Once the request to create a Single-use Certificate has been validated, the generation of the Certificate is immediate.

#### 4.2.3.2 [ORG CA] Organization Certificates

Once the request to create an Organization Certificate has been validated, the generation of the Certificate is carried out as soon as possible.
A specific technical document tracing the generation of the Certificate as well as the technical participants is created and kept as an execution log.

## 4.3 Issuance of the Certificate

### 4.3.1 Actions of the CA regarding the issuance of the Certificate

After authenticating the origin and verifying the integrity of the request from the Registration Authority, the CA initiates the process of generating the Certificate. The conditions for generating keys and Certificates and the security measures to be followed are specified in chapters 5 and 6 of this CP-CPS. Once generated, the CA transmits the Product Certificate to the Certificate Carrier Device via the RA. The Certificate Carrying Device guarantees the security of the Key Twins as defined in chapter 6.1.1.4.

#### 4.3.1.1 [OTU CA][OTU LCP CA] Single-use Certificates

In the case of Single-use Certificates, the Product Certificate is accessible to the Holder in the signature of the document(s) for which the Certificate was issued.

#### 4.3.1.2 [ORG CA] Organization Certificates

In the case of Organization Certificates, the issued Certificate is also sent to the Subscriber's representative to validate the information contained in the Certificate before it can be used (see chapter 4.4.1.2).

### 4.3.2 Notification by the CA of the issuance of the Certificate

The CA transmits the issued Certificate to the Certificate Carrier Device via the RA in response to the processing of the Certificate creation request (see chapter 4.3.1). The transaction is tracked in RA journals. Such transmission shall constitute notification.

#### 4.3.2.1 [OTU CA][OTU LCP CA] Single-use Certificates

Not applicable.

#### 4.3.2.2 [ORG CA] Organization Certificates

In the case of the issue of Organization Certificates, the Certificate is also sent to the Subscriber's representative (see chapter 4.3.1.2), which is equivalent to an express notification agreement.

## 4.4 Acceptance of the Certificate

### 4.4.1 Certificate acceptance process

#### 4.4.1.1 [OTU CA][OTU LCP CA] Single-use Certificates

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

Indeed, given the atomic nature of the signature operation in the context of the use of a Single-use Certificate, the validation of the data contained in the Certificate is carried out before it is issued.

In addition to this validation, automatic checks are carried out by the Certificate Carrier Device to detect any non-compliance before the Certificate is issued.

#### 4.4.1.2 [ORG CA] Organization Certificates

The Organization Certificate produced by the CA is sent to the Subscriber for validation before use as defined in chapter 4.3.1 this document.

The explicit acceptance of the information contained in the Certificate by either the legal or statutory representative of the Subscriber who made the request or the authorized individual identified in the Certificate is required by this CP-CPS within ten (10) business days of the generation of the Certificate (period called the "acceptance phase"). The explicit acceptance made by e-mail, the address of which is communicated when the subscription file is compiled, is considered sufficient. Indeed, the e-mail address of the issuer who was enrolled when the subscription file was created is deemed to be the authentication of the origin of the acceptance of the Certificate.

No use of Organization Certificates by the Certificate Carrying Device is possible without this acceptance phase.

Once this acceptance phase has expired, an issued Organizational Certificate is deemed accepted and can now be used by the Certificate Carrying Device.

### 4.4.2 Publication of the Certificate

There is no service for publishing Certificates issued by CAs. Only the Certificates of these CAs are published (see chapter2.2).

### 4.4.3 Notification by the CA to other entities of the issuance of the Certificate

Not applicable.

## 4.5 Uses of the Key pair and Certificate

### 4.5.1 Use of the private key and the Certificate by the Certificate Carrying Device

The use of the private key by the Certificate Carrier Device and the associated Certificate is strictly limited to the electronic signature/seal service as described in chapter 1.5.1.1 this document. Otherwise, MediaCert TSP cannot be held liable.

The authorized use of the Key pair and the associated Certificate is also indicated in the Certificate through the extensions concerning the use of the keys.

### 4.5.2 Use of the public key and Certificate by stakeholders

Subscribers must respect and ensure that their related persons requesting Certificates respect the use stipulated in the Certificates produced at their request by the CAs, as explained in chapter 4.5.1 above. They must therefore refuse any other use of the Certificate. Otherwise, the responsibility of Subscribers and persons related to them who have requested a Certificate may be engaged.

## 4.6 Renewal of a Certificate

Certificate renewal (new Certificate without key change) is not allowed under this CP-CPS.

### 4.6.1 Possible causes for renewal of a Certificate

Not applicable.

### 4.6.2 Origin of a renewal request

Not applicable.

### 4.6.3 Procedure for processing a renewal request

Not applicable.

### 4.6.4 Notification of the establishment of a new Certificate

Not applicable.

### 4.6.5 Acceptance process for the new Certificate

Not applicable.

### 4.6.6 Publication of the new Certificate

Not applicable.

### 4.6.7 Notification by the CA to other entities of the issuance of the new Certificate

Not applicable.

## 4.7 Issuance of a new Certificate following the change of the Key pair

The issuance of a new Certificate related to the generation of a new Key pair is treated as an initial request to create a Certificate.

It is prohibited to use an existing Key pair associated with an old CSR.

### 4.7.1 Possible reasons for changing a Key pair

Not applicable.

### 4.7.2 Origin of a request for a new Certificate

Not applicable.

### 4.7.3 Procedure for processing an application for a new Certificate

Not applicable.

### 4.7.4 Notification of the establishment of a new Certificate

Not applicable.

### 4.7.5 Acceptance process for the new Certificate

Not applicable.

### 4.7.6 Publication of the new Certificate

Not applicable.

### 4.7.7 Notification by the CA to other entities of the issuance of the new Certificate

Not applicable.

## 4.8 Modification of a Certificate

The modification of the Certificate is not authorized by this CP-CPS.

[ORG CA] However, the modification of an Organization Certificate is equivalent to revoking the Certificate in question and then proceeding to a new application for a Certificate according to the procedure described in chapter 4.1.1.2.

### 4.8.1 Possible reasons for modifying a Certificate

Not applicable.

### 4.8.2 Origin of a change request

Not applicable.

### 4.8.3 Procedure for processing a change request

Not applicable.

### 4.8.4 Acceptance procedure for the amended Certificate

Not applicable.

### 4.8.5 Publication of the amended Certificate

Not applicable.

### 4.8.6 Notification by the CA to other entities of the issuance of the amended Certificate

Not applicable.

## 4.9 Revocation and suspension of a Certificate

This CP-CPS does not authorize the suspension of the Certificate.

In addition, any information relating to the revocation of a CA's Certificate is available within the Certification Policy – Certification Practices Statements governing its issuing CA.

### 4.9.1 Possible reasons for revoking a Certificate

#### 4.9.1.1 [OTU CA][OTU LCP CA] Single-use Certificates

The following circumstances may lead to the revocation of a Holder's Single-use Certificate:

- the Certificate no longer complies with the CP-CPS to which it is subject;
- the cryptography used no longer ensures the connection between the subject and the public key;
- in the event of a major change, after impact assessment, affecting the validity of the Certificate;
- an incident occurred when the Certificate Carrier Device used the Holder's Certificate for a signature as part of normal use as defined in chapter 1.5.1.1;
- the private or public keys do not match or the Certificate Carrying Device is unable to use them for normal use as defined in chapter 1.5.1.1.

When one of the above circumstances occurs and the Certification Authority is aware of it, the Certificate in question must be revoked without delay. However, given the use of Single-use Certificates produced under this CP-CPS and the short lifespan of these Certificates, it is important to note that revocation is here primarily an instrument to provide a CRL for technical components that are required to dispose of them.

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

#### 4.9.1.2 [ORG CA] Organization Certificates

The following circumstances may lead to the revocation of the Certificate of Organization:

- the Certificate no longer complies with the CP-CPS to which it is subject;
- the cryptography used no longer ensures the connection between the subject and the public key;
- the Organization's information contained in the Certificate issued in its name is not in accordance with the identity of the Organization or the use intended in the Certificate;

- an error (intentional or unintentional) is detected in the Organization's application for registration;
- control over the use of the holder's private key is suspected lost or the holder's private key is:
  - suspected of compromise;
  - compromised;
  - lost;
  - volley;
  - destroyed;
  - altered.
- the authorized representative (see chapter 3.4.2 requests the revocation of the Certificate;
- termination of the activity of the Certification Authority , the Organization or the Subscriber;
- end of the contractual relationship between the Subscriber and the Certification Authority;
- change in technical or legal regulations, or change in recommendation applicable to the Certification Authority or the Organization, requiring the end of the use of the Certificate.

When one of the above circumstances occurs and the Certification Authority is aware of it, the Certificate in question must be revoked without delay.

In addition, the Certification Authority may automatically revoke an Organization Certificate in the following circumstances:

- non-compliance with this CP-CPS;
- non-compliance with any of the obligations arising from the subscriber contract or any other document in the subscription file (such as this CP-CPS and its chapter 9.6) by a Holder or a Subscriber, in particular concerning the use of the Certificate under conditions other than those provided for in this document (see chapter 1.5.1.1).

For this range of Certificate, the reason for revocation is published. This is one way to identify the type of Certificate in the CRL.

### 4.9.2 Origin of a revocation request

#### 4.9.2.1 [OTU CA][OTU LCP CA] Single-use Certificates

Only the Certificate Carrying Device is authorized to make a request for revocation of this type of Certificate following the encounter of one of the circumstances mentioned in chapter 4.9.1.1 of this document.

#### 4.9.2.2 [ORG CA] Organization Certificates

The persons and entities entitled to request revocation of this type of Certificate, following the encounter of one of the circumstances mentioned in chapter 4.9.1.2 of this document, are:

- the Subscriber's representative or one of the Subscriber's deputy representatives who has the identification and authentication data enabling him to access this function;
- the Certification Authority.

## 4.9.3 Procedure for processing a revocation request

### 4.9.3.1 [OTU CA][OTU LCP CA] Single-use Certificates

This CP-CPS does not require the identification of the revocation request. Indeed, only the Certificate Carrying Device as described in chapter 1.3.3 is able to request a revocation on the basis of one of the possible causes of revocation it has detected (see chapter 4.9.1.1).

The request is therefore automatically authorized. The CA then proceeds with the revocation. The operation is instantaneous and is recorded in the event logs (see chapter 5.4.1).

Once the Certificate is revoked, it cannot be reinstated. The subject concerned is informed of the change in status via the publication of the revoked Certificate in one of the Revoked Certificate Lists published at the address defined in chapter 2.2 this document.

### 4.9.3.2 [ORG CA] Organization Certificates

The request for revocation of this type of Certificate is not automatically authorized. Indeed, the request of the authorized person or entity (see chapter 4.9.1.2) must be validated by authorized Worldline personnel (called "Pilot"). For this purpose, the person or entity authorized to make the request contacts a telephone number provided to him when the Certificate subject to revocation was created. This number is available 7 days a week, 24 hours a day. The information to be provided to the Pilot for the authorization of the revocation is:

- identification details: name of the Organization and identity of the authorized representative;
- authentication element: secret code provided when creating the Certificate.

Once these elements have been validated by the system, the revocation request is then authorized. The operation is carried out in several steps by the Pilot. Some steps also require the intervention of the applicant, by telephone, who must give the information that the Pilot must enter or verify in order for the applicant to maintain control over the transaction. The operation is recorded in the event logs (see chapter 5.4.1).

Once the Certificate is revoked, it cannot be reinstated. The subject concerned is informed of the change in status via a notification sent by the RA and via the publication of the revoked Certificate in one of the Revoked Certificate Lists published at the address defined in chapter 2.2 this document.

A request for revocation of this type of Certificate is tracked and traced in order to comply with the revocation deadline set by the CA (see chapter 4.9.5.2).

However, the CA may revoke a Certificate (see chapter 4.9.2.2) if events so require. The [TDCP] provides more information on this subject.

### 4.9.4 Time allowed to make the request for revocation

#### 4.9.4.1 [OTU CA][OTU LCP CA] Single-use Certificates

Given the atomic nature of the operation in terms of computerized signature when using a Single-use Certificate, the request made by the applicant (see chapter 4.9.2.1) is immediate when one of the causes mentioned in chapter 4.9.1.1 is encountered.

#### 4.9.4.2 [ORG CA] Organization Certificates

As soon as the authorized representative becomes aware of one of the possible grounds for revocation defined in chapter 4.9.1.2 this document, he must make his request for revocation without delay.

### 4.9.5 Time for the CA to process a revocation request

The maximum time between receipt of the revocation request and consideration of the revocation request is twenty-four (24) hours, with the revocation management function available 7 days a week, 24 hours a day.

#### 4.9.5.1 [OTU CA][OTU LCP CA] Single-use Certificates

The request to revoke a Single-use Certificate is processed immediately after it is received by the CA. Revocation is effective when the Certificate in question is introduced into the generated CRL.

The operation is immediately and automatically carried out after receipt and validation of the request.

#### 4.9.5.2 [ORG CA] Organization Certificates

The request to revoke an Organizational Certificate is processed immediately after it is received by the OTU CA. Revocation is effective when the Certificate in question is introduced into the generated CRL.

A request for revocation of an Organizational Certificate being defined by its number tracked and by its revocation date, its tracking and traceability are clearly defined and achievable. This makes it possible to check whether the revocation deadline has been respected or not.

### 4.9.6 Requirements for verification of revocation by Certificate users

#### 4.9.6.1 [OTU CA][OTU LCP CA] Single-use Certificates

When using a Single-use Certificate provided by an online CA, this CP-CPS does not formulate, given the computer atomic nature of the signature operation, any requirement for verification of the revocation of the Certificate.

#### 4.9.6.2 [ORG CA] Organization Certificates

When using an Organizational Certificate provided by the OTU CA, the user must check the status of the Certificate they intend to rely on before using it. To do this, he can either consult the published CRLs or make a request to the OCSP answering machine (see chapter 4.10).

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

### 4.9.7 Frequency of establishment of CRL

The frequency of establishment of CRL is twenty-four (24) hours. However, a new CRL may be published at any time, following a revocation for example. They are valid for seven (7) days.

### 4.9.8 Maximum time limit for publication of a CRL

A CRL shall be published within a maximum period of sixty (60) minutes following its generation.

### 4.9.9 Availability of an online system for checking the revocation and status of Certificates

An OCSP answering machine is made available online and is accessible as described in chapter 2.2, allowing the user to check the revocation and status of Certificates online (see chapter 4.10).

The revocation information made available is consistent between the different revocation information services (CRL and OCSP answering machine).

### 4.9.10 Online verification requirements for user revocation of Certificates

The online verification requirements for the revocation of Certificates by users are as detailed in chapter 4.9.6 this CP-CPS.

### 4.9.11 Other available means of information on revocations

Not applicable.

### 4.9.12 Specific requirements in the event of compromise of the private key

Entities authorized to make a revocation request are required to do so as soon as possible after becoming aware of the compromise of the private key (see chapter 4.9.4).

With regard to CA Certificates, revocation following a compromise of the private key will be notified to the inspection body [ANSSI Notification] within twenty-four (24) hours in accordance with the requirements of [eIDAS].

### 4.9.13 Possible causes of a suspension

Under this CP-CPS, suspension of Certificates is not permitted.

### 4.9.14 Origin of a request for suspension

Not applicable.

### 4.9.15 Procedure for processing a request for suspension

Not applicable.

### 4.9.16 Limits on the period of suspension of a Certificate

Not applicable.

## 4.10 Certificate Status Information Functions

### 4.10.1 Operational characteristics

CAs provide users with two mechanisms for public consultation of the Certificate status: CRLs and the OCSP answering machine.
CRLs are published in v2 format on the Internet, accessible in HTTP protocol(s) at:

- specified in chapter 2.2 this CP-CPS;
- specified in the Certificate issued by the issuing CA as specified in chapter 7.1 this CP-CPS.

A CRL contains a list of Certificates issued by one of the online CAs that are both revoked and unexpired (date and time of expiry of the Certificate not reached). Indeed, a revoked and expired Certificate no longer appears in the LCR. It shall contain in particular the date of its publication and the date of the next publication.
The CRLs are also signed by the OTU CA to ensure their origin and integrity.
The link to the OCSP answering machine is specified on the Internet, accessible in HTTP protocol (s) at the address:

- specified in chapter 2.2 this CP-CPS;
- specified in the Certificate issued by the issuing CA as specified in chapter 7.1 this CP-CPS.

The CAs ensure the origin and integrity of the responses provided by the OCSP answering machine that it makes available to users.

### 4.10.2 Availability of the function

The Certificate status information function is available 7 days a week, 24 hours a day. The maximum downtime of the platform is eight (8) hours per month.

### 4.10.3 Optional devices

Not applicable.

## 4.11 End of the relationship between the Subscriber and the CA

The termination of the relationship between the Subscriber and MediaCert TSP as part of the services presented in chapter1.5.1.1 shall take the form of the termination or non-renewal of the Subscription Contract or the service contracts expressly linked to it.

The Registration Authority no longer recognizes requests transmitted and signed by the Subscriber, his representative or his representative's deputies.

The Subscriber is then requested to make one or more requests (taking into account the number of Certificates concerned) to revoke his or her Organizational Certificate(s) without delay if they are still valid.

## 4.12 Key escrow and recovery

The escrow of private keys of CAs and Bearer Certificates is prohibited by this CP-CPS.

### 4.12.1 Key escrow collection policy and practices

Not applicable.

### 4.12.2 Session key encapsulation recovery policy and practices

Not applicable.

# 5 Non-technical security measures

## 5.1 Physical security measures

### 5.1.1 Geographical location and site construction

All requirements and practices described in the [GP] apply.

In particular, all premises hosting systems involved in the generation and revocation of Certificates are operated in an environment that physically protects services from threats of compromise due to unauthorized access to systems or data. The perimeter of the secure area is clearly identified and cannot be accessed by unauthorized personnel or third party organizations.

### 5.1.2 Physical access

All requirements and practices described in the [GP] apply.

### 5.1.3 Power supply and air conditioning

All requirements and practices described in the [GP] apply.

### 5.1.4 Vulnerability to water damage

All requirements and practices described in the [GP] apply.

### 5.1.5 Fire prevention and protection

All requirements and practices described in the [GP] apply.

### 5.1.6 Conservation of the supports

All requirements and practices described in the [GP] apply.

### 5.1.7 Decommissioning of supports

All requirements and practices described in the [GP] apply.

### 5.1.8 Off-site Backups

All requirements and practices described in the [GP] apply.

## 5.2 Procedural security measures

### 5.2.1 Trusted roles

All requirements and practices described in the [GP] apply.

### 5.2.2 Number of people required

All requirements and practices described in the [GP] apply.

### 5.2.3 Identification and authentication for each role

All requirements and practices described in the [GP] apply.

### 5.2.4 Roles requiring segregation of duties

All requirements and practices described in the [GP] apply.

## 5.3 Security measures for staff

### 5.3.1 Required qualifications, skills and authorizations

All requirements and practices described in the [GP] apply.

### 5.3.2 Background check procedures

All requirements and practices described in the [GP] apply.

### 5.3.3 Initial training requirements

All requirements and practices described in the [GP] apply.

### 5.3.4 Continuing education requirements and frequency

All requirements and practices described in the [GP] apply.

### 5.3.5 Frequency and sequence of rotation between different allocations

All requirements and practices described in the [GP] apply.

### 5.3.6 Sanctions in the event of unauthorized actions

All requirements and practices described in the [GP] apply.

### 5.3.7 Requirements for the staff of external service providers

All requirements and practices described in the [GP] apply.

### 5.3.8 Documentation provided to staff

All requirements and practices described in the [GP] apply.

## 5.4 Procedures for compiling audit data

### 5.4.1 Type of recorded events

All requirements and practices described in the [GP] apply.

In addition to the events described in the |GP], this policy requires CAs within its scope to collect the following audit data:

- all security-related events, in particular:
    - physical access to the premises hosting the systems;
    - changes in system security policy;
    - changes in personnel working on behalf of CAs;
    - system starts and stops;
    - the start and stop of the logging function parameters;
    - hardware and software failures;
    - modifications (change, correction or evolution) of the various components;
    - attempts to access systems;
    - connections and disconnections to the systems of authorized users.
- all events relating to the registration of holders, in particular:
    - receipt of a Certificate application (initial and renewal);
    - validation / rejection of a Certificate request;
    - events related to signature keys and CA Certificates (generation (key ceremony), backup / recovery, revocation, renewal, destruction, etc.) ;
    - generation of Bearer Certificates ;
    - publication and updating of CA-related information (CP-CPS, CA Certificates, general conditions of use, etc.);
    - receipt of a revocation request;
    - validation / rejection of a revocation request;
    - generation and publication of LAR and LCR.

Regarding the registration procedure, the CAs also keep:

- the identity of the person who applied for the Certificate;
- the original of the Certificate application form;
- the identity of the person in a trusted role who made the recording.

As the registration file contains the holder's personal data, storage is subject to security measures in accordance with chapter 9.4 this document.

### 5.4.2 Frequency of event log processing

All requirements and practices described in the [GP] apply.

### 5.4.3 Event log retention period

Event logs intended to be kept are archived. The archiving period for this information is specified in chapter 5.5.2 this document.

### 5.4.4 Protection of event logs

Event logs are protected under the same conditions as those defined in chapter 5.5.3 this document.

### 5.4.5 Procedure for backing up event logs

The procedure for backing up online CAs event logs is internal and specified in the [TDCP] document.

### 5.4.6 Event log collection system

Online CAs event log collection system is internal and specified in the [TDCP] document.

### 5.4.7 Notification of the registration of an event to the event manager

All requirements and practices described in the [GP] apply.

### 5.4.8 Vulnerability assessment

Vulnerabilities are assessed during a risk analysis (see chapter on risk analysis in the [GP]). The control of functional event logs is carried out on demand in the event of a dispute, or for analysis of the PKI's behaviour.

## 5.5 Data Archiving

Archiving arrangements are put in place by MediaCert TSP. This archiving ensures the durability of the journals constituted by the various components of the PKI.

### 5.5.1 Types of data to be archived

The data to be archived are as follows:

- software (executable) and configuration files of computer equipment;
- CP-CPS;
- TDCP;

- registration files;
- the Certificates issued;
- LARs and CRLs issued or published;
- the various commitments signed by the MediaCert Committee;
- the event logs of the different PKI entities (see chapter 5.4.1).

### 5.5.2 Archive retention period

The minimum retention periods are as follows:

| Version | Author(s) |
|---|---|
| **3 years** after the end of the CA's life | • software (executable) and configuration files of computer equipment;<br>• CP-CPS;<br>• TDCP;<br>• the Certificates issued;<br>• LARs and CRLs issued or published;<br>• the various commitments signed by the MediaCert Committee. |
| **7 years** after the expiry of the associated Certificate | • registration files;<br>Note: Specificity for registration files related to Single-use Certificates, the retention period of the archive is eight (8) years, due to the special nature of the lifetime of this range of Certificates.<br>• the elements of the Certificate life cycle (generation, revocation,...). |
| **10 years** after their generation | Other audit data (e.g. system start-ups and shutdowns) |

However, the storage period for registration files may be modified at the request of the Subscriber, who may request an extension beyond the period defined above from Worldline, by express agreement under specific conditions of the Subscription Contract. This extension must be justified by regulatory or legal constraints and accompanied by an obligation to inform the Subscriber of the persons concerned by the processing of personal data contained in the registration file.

### 5.5.3 Protection of archives

All requirements and practices described in the [GP] apply.

The means of archive protection implemented by MediaCert TSP in the context of online CAs differ according to the type of data. Typically:

- digital documentary archives are protected by a digital safe whose access is controlled by MediaCert TSP.
- handwritten archives are protected by secure physical systems such as safes or strong cabinets, access to which is controlled by the MediaCert TSP.

### 5.5.4 Archive backup procedure

All requirements and practices described in the [GP] apply.

### 5.5.5 Data time stamping requirements

Chapter 6.8 this document specifies the requirements for dating, timestamping.

### 5.5.6 Archive collection system

All requirements and practices described in the [GP] apply.

### 5.5.7 Procedure for retrieving and verifying archives

The procedure for retrieving CA archives is internal and is specified in the [TDCP]. Access to the archives is subject to restrictions.

The archives will be made available in case of judicial requisition.

## 5.6 Change of CA Key pair

CAs may not generate a Certificate with an end date later than the expiry date of the corresponding CA Certificate. For this purpose, the period of validity of the CA Certificate must be longer than that of the Certificates it signs.

With regard to the expiry date of this Certificate, its renewal will be requested within a period at least equal to the lifetime of the Certificates signed by the corresponding private key.

As soon as a new CA Key pair is generated, only the new private key will be used to sign Certificates.

The previous Certificate remains usable to validate Certificates issued under this key until all Certificates signed with the corresponding private key have expired.

## 5.7 Recovery from compromise and disaster

### 5.7.1 Procedures for reporting and handling incidents and compromises

All requirements and practices described in the [GP] apply.

In the case of a major incident, such as loss, suspicion of compromise, compromise, theft of a CA' s private key, the triggering event is the recognition of this incident at the PKI level. The person in charge of the MediaCert TSP must be informed immediately. He will then have to ensure that the anomaly is treated. If he considers that the incident is of a serious nature, he will request an immediate revocation of the Certificate. If this occurs, it will publish the information of revocation

of the Certificate in the greatest urgency, or even immediately. It will do so via the MediaCert TSP public website and/or via e-mail notification to all customers. If any of the algorithms, or associated parameters, used by the CA or its bearers become insufficient for its remaining intended use, then the MediaCert TSP manager will publish the information via the public site and notify all of its affected customers by email. All relevant Certificates will then be revoked.

### 5.7.2 Recovery procedures in case of corruption of IT resources (hardware, software and/or data)

MediaCert TSP has a business continuity plan (see chapter 5.7.4) to meet the availability requirements of the various PKI functions arising from this CP-CPS, the CAs' online commitments in this CP-CPS, in particular with regard to functions related to the publication and/or revocation of Certificates. This plan is regularly tested.

### 5.7.3 Recovery procedures in case of compromise of a component's private key

The compromise of an infrastructure or component control key is addressed in the component's continuity and disaster recovery plan (see chapter 5.7.4) disaster.

In the event of a compromise of the CA private key, the MediaCert TSP will publicly indicate that Certificates and revocation information issued using that key may no longer be valid. The relevant Certificate will be immediately revoked.

### 5.7.4 Continuity capacities following a disaster

All requirements and practices described in the [GP] apply.

## 5.8 End of life of the PKI

The cessation of activity may be total or partial (for example: cessation of activity for a given family of Certificates only).

The partial cessation of activity will be gradual so that only the obligations referred to below are to be performed by the PKI, or a third party entity that takes over the activities, upon expiry of the last Certificate issued.

In the event of a total cessation of activity, the PKI or, in the event of impossibility, any entity that would be substituted for it by virtue of a law, regulation, court decision or agreement previously concluded with this entity, must ensure the revocation of the Certificates and the publication of the LAR/LCR in accordance with the commitments made in its CP-CPS. A cessation of activity plan is then applied by the PKI. This plan is regularly updated and includes the actions listed below.

The PKI shall take the following measures in the event of cessation:

- notification of affected entities;
- the transfer of its obligations to Worldline;
- managing the revocation status for unexpired Certificates that have been issued.

When the service is stopped, the PKI will take the following measures:

- inform (for example by receipt) all holders of revoked or to be revoked Certificates, as well as their connecting entities if applicable;
- refrain from transmitting the private key that enabled him to issue Certificates;
- revoke all the Certificates it has signed and which are still valid;
- revoke its Certificate;
- take all necessary measures to destroy it or render it inoperative (the nominal key and any backups).

# 6 Technical security measures

## 6.1 Generation and installation of Key pairs

### 6.1.1 Generation of Key pairs

#### 6.1.1.1 CA Key pairs

All requirements and practices described in the [GP] apply.

Online CA signing keys are generated and implemented in a cryptographic module that has undergone a security assessment as defined in chapter 6.2.11.1 this document.
These signature keys have a unique identifier that is necessarily specified when configuring applications so as not to compromise their use.

#### 6.1.1.2 Authentication keys of a TGI component

All requirements and practices described in the [GP] apply.

#### 6.1.1.3 Subscriber Authentication Keys

Subscriber authentication is described in chapter 3.2.5 this CP-CPS.

Online CAs do not produce Authentication Certificates attached to a Subscriber's private key and are not responsible for issuing these Certificates. Indeed, the Subscriber is informed of the rules to be respected in order to authenticate himself with the Registration Authority (see chapter 3.2.5) and it is up to him to obtain the Certificate(s) allowing him to authenticate himself with the RA.

#### 6.1.1.4 Key pairs of Bearer Certificates generated by the CA

Online CA do not generate the keys of the Bearer Certificates.

#### 6.1.1.5 Key pairs of Bearer Certificates generated for the Stakeholder

The Key pairs are generated by the Certificate Carrying Device, which retains exclusive use of them, under the following conditions:

| Single-use Certificate | Certificate of Organization |
|---|---|
| Within a physically isolated cryptographic module meeting the requirements defined in chapter 6.2.11.2 this document | |
| Copied onto other dedicated cryptographic modules intended for the same use, meeting the same requirements as above, according to the cloning processes recommended by the supplier | |
| In the secure premises of the MediaCert TSP (see chapter 5.1) | |
| Under the control of the Certificate Carrying | |

| Single-use Certificate | Certificate of Organization |
|---|---|
| Device | Under the supervision of two (2) persons in a trusted role within the MediaCert TSP |
| According to a script previously defined by the MediaCert TSP | According to an Organizational document and a technical document both signed by all the participants, in particular by the master of ceremonies |

Control and protection measures are implemented by the MediaCert TSP at the Certificate Carrier Device level to protect the use of private keys.

It is also prohibited by this CP-CPS to use an existing Key pair associated with a former CSR (see chapter 4.7).

### 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 public key is transmitted by the Certificate Carrier Device to the Registration Authority, which transmits it to the target CA within a template in PKCS#10 (CSR) format for the generation of the Single-use/Organization Certificate.

### 6.1.4 Transmission of the CA public key to Certificate users

Certificates containing CA public keys are published on its website, the address of which is defined in chapter 2.2 this document.

### 6.1.5 Key pair size

All requirements and practices described in the [GP] apply.

The specific additional requirements and practices defined below also apply.

| Key pairs | Algorithm | Hash function | Size (bits) |
|---|---|---|---|
| OTU CA Certificates | RSA | SHA-2 | 4096 |
| OTU LCP CA Certificates | RSA | SHA-2 | 4096 |
| ORG CA Certificates | RSA | SHA-2 | 4096 |
| Single-use "standard" Certificates | RSA | SHA-2 | 2048 |
| Single-use "reinforced" Certificates | RSA | SHA-2 | 2048 |
| Organization Certificates | RSA | SHA-2 | 2048 |
| Single-use "standard" test Certificates | RSA | SHA-2 | 2048 |
| Single-use "reinforced" test Certificates | RSA | SHA-2 | 2048 |

| Key pairs | Algorithm | Hash function | Size (bits) |
|---|---|---|---|
| Test Organization Certificates | RSA | SHA-2 | 2048 |

### 6.1.6 Verification of the generation of Key pair parameters and their quality

The Key pair generation equipment used for the generation of CA Key pair parameters is cryptographic modules configured to meet these requirements (see chapter 6.1.1.1). The Key pairs can only be generated on a module that complies with this requirement, or at a higher cryptographic and security level.

The same applies to the bearer Key pairs (see chapter 6.1.1.5).

### 6.1.7 Objectives of the key use

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

## 6.2 Security measures for private key protection and cryptographic modules

### 6.2.1 Standards and security measures for cryptographic modules

#### 6.2.1.1 CA Cryptographic Modules

All requirements and practices described in the [GP] apply.

CA signature keys are generated and implemented in a cryptographic module that has undergone a security assessment as defined in chapter 6.2.11.1 this document.
However, the signature keys of these CAs are operated in separate software components to ensure control during use.

#### 6.2.1.2 Beneficiaries' cryptographic devices

Not applicable.

### 6.2.2 Checking the private key

#### 6.2.2.1 CA private keys

All requirements and practices described in the [GP] apply.

In addition, the control of CA private signing keys is carried out by trusted personnel (secret holders) and via a tool implementing secret sharing.

#### 6.2.2.2 Private keys of the Bearer Certificates

The control of the private keys corresponding to the different Certificates issued by the CAs is ensured by the Certificate Carrier Device, which has exclusive control over them. However, this exclusive control remains subject to the activation described in chapter 6.4.1.2 this document.

### 6.2.3 Private key escrow

All requirements and practices described in the [GP] apply.

### 6.2.4 Backup copy of the private key

All requirements and practices described in the [GP] apply.

In addition, as the private keys of CAs governed by this CP-CPS are not permanently activated within the cryptographic module, these private keys are backed up outside a cryptographic module. This backup copy is made in encrypted form and with an integrity control mechanism. The encryption used provides a level of security equivalent to or greater than the storage within the cryptographic module and, in particular, is based on an algorithm, key length and operating mode capable of resisting cryptanalytic attacks for at least the lifetime of the key thus protected. Encryption and decryption operations are performed within the cryptographic module in such a way that CA private keys are at no time in clear text outside the cryptographic module. The storage media for backup copies are stored in a safe. The control of encryption/decryption operations complies with the requirements of chapter 6.2.2.

### 6.2.5 Archiving the private key

All requirements and practices described in the [GP] apply.

### 6.2.6 Transfer of the private key to/from the cryptographic module

#### 6.2.6.1 CA private keys

The transfer to/from the cryptographic module is only done for the generation of backup copies. This is done in numerical form, in accordance with the requirements of chapter 6.2.4

#### 6.2.6.2 Private keys of the Bearer Certificates

Not applicable.

### 6.2.7 Storage of the private key in a cryptographic module

All requirements and practices described in the [GP] apply.

### 6.2.8 Method of activating the private key

#### 6.2.8.1 CA private keys

All requirements and practices described in the [GP] apply.

#### 6.2.8.2 Private keys of the Bearer Certificates

##### [OTU CA][OTU LCP CA] Single-use Certificates

The private keys of Single-use Certificates are activated by the Certificate Carrier Device with one of the cryptographic modules provided for this purpose, after receipt of the Single-use Certificate issued by the target CA during the signature session.

#### [ORG CA] Organization Certificates

The private keys of the Organization Certificates are activated by the Certificate Carrier Device with one of the cryptographic modules provided for this purpose, after receipt of a duly validated and authenticated request.

### 6.2.9 Method of deactivating the private key

#### 6.2.9.1 CA private keys

All requirements and practices described in the [GP] apply.

#### 6.2.9.2 Private keys of the Bearer Certificates

##### [OTU CA][OTU LCP CA] Single-use Certificates

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

##### [ORG CA] Organization Certificates

The deactivation of the private key of an Organization Certificate in the cryptographic module is automatic as soon as the sealing operation session ends or as soon as the module is stopped or disconnected.

### 6.2.10 Method of destroying the private key

#### 6.2.10.1 CA private keys

All requirements and practices described in the [GP] apply.

In addition, the permanent destruction of a CA private key is achieved by destroying the means of restoring the private key:

- the destruction of the private key and all backup copies, and
- the destruction of the means of activation of the private key if applicable.

#### 6.2.10.2 Private keys of the Bearer Certificates

##### [OTU CA][OTU LCP CA] Single-use Certificates

The private keys of Single-use Certificates are destroyed after their use by the Certificate Carrier Device, which then tracks the event.

##### [ORG CA] Organization Certificates

Not applicable.

### 6.2.11 Qualification level of the cryptographic module

#### 6.2.11.1 Cryptographic modules associated with CA Certificates

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

#### 6.2.11.2 Cryptographic modules associated with Bearer Certificates

The hardware cryptographic module used to host the private keys of the Subscriber Certificates generated by the CAs is evaluated at the following Certification level: FIPS 140-2 level 3.

## 6.3 Other aspects of Key pair management

### 6.3.1 Public key archiving

CA public keys are archived in accordance with chapter 5.5.2 this document.

### 6.3.2 Lifetime of Key pairs and Certificates

The lifetime of Key pairs and Certificates differs according to the type of Certificate. The size of the Key pairs has been taken into account when defining these service lives, in accordance with cryptographic requirements [ETSI TS 119 312].

CAs may not issue Bearer Certificates whose lifetime exceeds that of the CA Certificate used for the issue.

| Key pairs | Life expectancy |
|---|---|
| OTU CA Certificates | 10 years old |
| OTU LCP CA Certificates | 10 years old |
| ORG CA Certificates | 10 years old |
| Single-use "standard" Certificates | 15 minutes |
| Single-use "reinforced" Certificates | 15 minutes |
| Organization Certificates | 3 years |
| Single-use "standard" test Certificates | 15 minutes |
| Single-use "reinforced" test Certificates | 15 minutes |
| Test Organization Certificates | 3 years |

### 6.3.3 Key pair inventory

#### 6.3.3.1 Key pairs and CA Certificates

MediaCert TSP maintains a regularly updated inventory of secrets and Key pairs.

#### 6.3.3.2 Key pairs and bearer Certificates

An inventory is carried out in order to verify that all private keys produced by CAs for the Certificate Carrier Device have been properly requested.

## 6.4 Activation data

### 6.4.1 Generation and installation of activation data

#### 6.4.1.1 Generation and installation of activation data corresponding to the private key of a CA

All requirements and practices described in the [GP] apply.

#### 6.4.1.2 Generation and installation of activation data corresponding to the private key of a Bearer Certificate

There is no activation data corresponding to the private key of a Bearer Certificate. However, the Certificate Carrier Device may not use the private key of a Bearer Certificate without having received a request from the Subscriber.

### 6.4.2 Activation data protection

#### 6.4.2.1 Protection of activation data corresponding to the private key of a CA

All requirements and practices described in the [GP] apply.

#### 6.4.2.2 Protection of activation data corresponding to the private key of a Bearer Certificate

A protection of the authentication mechanism of the Certificate Carrier Device for the activation and use of private keys is implemented.

## 6.5 Computer system security measures

### 6.5.1 Technical security requirements specific to computer systems

All requirements and practices described in the [GP] apply.

### 6.5.2 Qualification level of computer systems

Not applicable.

## 6.6 Security measures for systems during their life cycle

### 6.6.1 Security measures related to system development

All developments carried out by the MediaCert TSP and impacting the PKI are documented and carried out via a process in order to ensure their quality. The system configuration of the PKI components and any modifications and upgrades are documented and controlled. In addition, MediaCert TSP operates a partitioning between development, testing, pre-production and production environments. This ensures a quality production start.

### 6.6.2 Measures related to safety management

Any system evolution of a PKI component is documented and tracked. It appears in the internal operating procedures of the component.

### 6.6.3 Level of security assessment of the life cycle of systems

Any significant system evolution of a PKI component is tested and validated before deployment. These operations are carried out by trusted personnel.

## 6.7 Network security measures

All requirements and practices described in the [GP] apply.

## 6.8 Time-stamping / Dating system

All requirements and practices described in the [GP] apply.

In addition, MediaCert TSP servers synchronize their internal clocks at most every 24 hours on reference servers to ensure the consistency of the time (UTC) indicated in the various electronic logs.

# 7 Certificate and CRL Profile

## 7.1 Certificate Profiles

### 7.1.1 Definitions of the terms

Certificates issued by online CAs, including their 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 issuing CA to sign the issued Certificate |
| Issuer | Value of the DN (X.500) of the CA issuing the Certificate |
| Validity | Date of activation and expiry of the Certificate |
| Subject | Value of the DN (X.500) of the subject |
| Subject Public Key Key Info | Algorithm OID and public key value |
| Extensions | List of extensions.<br>An extension can be critical or non-critical:<br>• if it is critical, the user application to which the Certificate is presented must be able to process it in accordance with its use. If the application does not know how to handle the extension or if the extension is not in accordance with its expected use, it must reject the Certificate;<br>• if it is non-critical, there is no Certificate rejection and the application may ignore the extension in question. |

### 7.1.2 Certificate of the OTU CA

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

| DN Fields | Mandatory | Description |
|---|---|---|
| **C** | Yes, it is. | Country of the Organization governing the CA: FR |
| **O** | Yes, it is. | Legal name of the Organization governing the CA: Worldline |
| **OU** | Yes, it is. | Organizational identifier governing the CA: 0002 378901946 |
| **SERIALNUMBER** | Yes, it is. | Unique serial number of the DN [1] |
| **CN** | Yes, it is. | Identity of the holder: MediaCert OTU CA 2019 |

#### 7.1.2.1 Base fields

| Fields | Value |
|---|---|
| **Version** | 2 (for version 3) |
| **Serial number** | Automatically generated during the Key Ceremony |
| **Signature** | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | DN of the issuing CA (see chapter 1.2.2) |
| **Validity** | 10 years old |
| **Subject** | DN of the Technical CA (see chapter 7.1.2) |
| **Subject Public Key Info** | RSA 4096 bits |

#### 7.1.2.2 Extensions

| Fields | Criticism | Value |
|---|---|---|
| **Authority Key Identifier** | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | Yes, it is. | keyCertSign, CRLSign |
| **Certificate Policies** | No | • Policy Identifier : anyPolicy (2.5.29.32.0)<br>• Policy Qualifier Id: 1.3.6.1.5.5.7.2.1<br>• Qualifier: https://www.mediacert.com |
| **Basic Constraint** | No | • CA: true<br>• Maximum Path Length 0 |
| **CRL Distribution Points** | No | • fullName : http://www.mediacert.com/trustCA2019/trustCA2019.crl [2] |

[1] This SERIALNUMBER is used to differentiate between the different TCAs. This is an incremented counter each time a new TCA is issued. It is constructed as follows:

SERIALNUMBER =

- *1:* represents the Technical Certification Authority 1;
- *2:* represents the Technical Certification Authority 2;
- …

| Fields | Criticism | Value |
|---|---|---|
| | | • reason: Absent<br>• cRLIssuer: Absent |
| **Authority Information Access** | No | • accessMethod : id-ad-caIssuers<br>• accessLocation: http://www.mediacert.com/trustCA2019/trustCA2019.crt [2] |

### 7.1.3 Certificate of the OTU LCP CA

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

| DN Fields | Mandatory | Description |
|---|---|---|
| **C** | Yes, it is. | Country of the Organization governing the CA: FR |
| **O** | Yes, it is. | Legal name of the Organization governing the CA: Worldline |
| **OU** | Yes, it is. | Organizational identifier governing the CA: 0002 378901946 |
| **SERIALNUMBER** | Yes, it is. | Unique serial number of the DN [3] |
| **CN** | Yes, it is. | Identity of the holder: MediaCert OTU LCP CA 2018 |

#### 7.1.3.1 Base fields

| Fields | Value |
|---|---|
| **Version** | 2 (for version 3) |
| **Serial number** | Automatically generated during the Key Ceremony |
| **Signature** | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | DN of the issuing CA (see chapter 1.2.2) |
| **Validity** | 10 years old |
| **Subject** | DN of the Technical CA |
| **Subject Public Key Info** | RSA 4096 bits |

#### 7.1.3.2 Extensions

| Fields | Criticism | Value |
|---|---|---|
| **Authority Key Identifier** | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | Yes, it is. | keyCertSign, CRLSign |

[3] This SERIALNUMBER is used to differentiate between the different TCAs. This is an incremented counter each time a new TCA is issued. It is constructed as follows:
[3] This SERIALNUMBER is used to differentiate between the different TCAs. This is an incremented counter each time a new TCA is issued. It is constructed as follows:
SERIALNUMBER =
- *1:* represents the Technical Certification Authority 1;
- *2:* represents the Technical Certification Authority 2;
- …

| Fields | Criticism | Value |
|---|---|---|
| **Certificate Policies** | No | • Policy Identifier : anyPolicy (2.5.29.32.0)<br>• Policy Qualifier Id: 1.3.6.1.5.5.7.2.1<br>• Qualify: https://www.mediacert.com |
| **Basic Constraint** | No | • CA: true<br>• Maximum Path Length : 0 |
| **CRL Distribution Points** | No | • fullName: http://www.mediacert.com/rootCA2018/rootCA2018.crl [4]<br>• reason : Absent<br>• cRLIssuer : Absent |
| **Authority Information Access** | No | • accessMethod : id-ad-caIssuers<br>• accessLocation: http://www.mediacert.com/rootCA2018/rootCA2018.crt [4] |

[4] This URL is given for information only. The authentic URL is the one in the Certificate.

### 7.1.4 ORG CA Certificate

ORG CA Certificates, called Technical CA Certificates (ACT), are differentiated by the Serial Number (SERIALNUMBER) field of the Subject's Distinguished Name (DN).

| 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 | Organizational identifier governing the CA: 0002 378901946 |
| **SERIALNUMBER** | Yes | Unique serial number of the DN [5] |
| **CN** | Yes | Identity of the holder: MediaCert ORG CA 2018 |

#### 7.1.4.1 Base fields

| Fields | Value |
|---|---|
| **Version** | 2 (for version 3) |
| **Serial number** | Automatically generated during the Key Ceremony |
| **Signature** | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | DN of the issuing CA (see chapter 1.2.2) |
| **Validity** | 10 years old |
| **Subject** | DN of the AC Technique |
| **Subject Public Key Info** | RSA 4096 bits |

#### 7.1.4.2 Extensions

| Fields | Critical | Value |
|---|---|---|
| **Authority Key Identifier** | No | [RFC 5280] method [0] : public key identifier of the issuing CA |
| **Subject Key Identifier** | No | [RFC 5280] method [1] : identifier of the public key contained in the Certificate |
| **Key Usage** | Yes | keyCertSign, CRLSign |
| **Certificate Policies** | No | • Policy Identifier : anyPolicy (2.5.29.32.0)<br>• Policy Qualifier Id : 1.3.6.1.5.5.7.2.1<br>• Qualifier : https://www.mediacert.com |
| **Basic Constraint** | No | • CA : true<br>• Maximum Path Length : 0 |
| **CRL Distribution Points** | No | • fullName : http://www.mediacert.com/trustCA2019/trustCA2019.crl [6] |

[5] This SERIALNUMBER is used to differentiate between the different TCAs. This is an incremented counter each time a new TCA is issued. It is constructed as follows:

SERIALNUMBER =

- *1:* represents the Technical Certification Authority 1;
- *2:* represents the Technical Certification Authority 2;

...

[6] This URL is given for information only. The authentic URL is the one in the Certificate.

| Fields | Critical | Value |
|---|---|---|
| | | • reason : Absent<br>• cRLIssuer : Absent |
| **Authority Information Access** | No | • accessMethod : id-ad-caIssuers<br>• accessLocation: http://www.mediacert.com/trustCA2019/trustCA2019.crt [6] |

### 7.1.5 Single-use "standard" Certificate

#### 7.1.5.1 Base fields

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the issuing Technical CA |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **Validity** | | 15 minutes |
| **Subject** | C | Nationality of the Holder |
| | SN | Name of the Holder |
| | GN | First name of the Holder |
| | OU | Subscriber's name |
| | SERIALNUMBER [7] | Unique DN serial number |
| | CN | Identity of the holder trained in such a way:<br>First name of the Holder [space] Name of the Holder [space] [TraceID] [8] |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.1.5.2 Extensions

| Fields | | Criticism | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | [RFC 5280] method [0] : public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | | Yes, it is. | nonRepudiation |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3.5 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | https://www.mediacert.com |

[7] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime:* represents the time of request of the Certificate;
- *DocRef:* represents the identification of the document to be signed (in case of multi-signature, it is the first document that is referenced in the signature request that appears);
- *ClientId*: represents the unique identification of the client.

*The ReqTime* value is used to protect against a case of co-signatures by two (2) people with the same name. The concatenation of the three (3) information guarantees a unique value among all users.

[8] Represents the unique identification of the trace container for the signature.

| Fields | | Criticism | Value |
|---|---|---|---|
| **CRL Distribution Points** | | No | http://pki-otu-lcp-ac[SERIALNUMBER TCA issuer].mediacert.com/crl [9] |
| **Authority Information Access** | ocsp | No | http://pki-otu-lcp-ac[SERIALNUMBER TCA issuer].mediacert.com/ocsp [7] |
| | caIssuers | | http://pki-otu-lcp-ac[SERIALNUMBER TCA issuer].mediacert.com/certificate [7] |

## 7.1.6 Single-use "reinforced" Certificate

### 7.1.6.1 Base fields

| Fields | | Value |
|---|---|---|
| Version | | 2 (for version 3) |
| Serial number | | Defined by the issuing Technical CA |
| Signature | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Issuer | | DN of the issuing Technical CA |
| Validity | | 15 minutes |
| Subject | C | Nationality of the Holder |
| | SN | Name of the Holder |
| | GN | First name of the Holder |
| | OU | Subscriber's name |
| | SERIALNUMBER [10] | Unique DN serial number |
| | CN | Identity of the holder trained in such a way:<br>First name of the Holder [space] Name of the Holder [space] [TraceID] [11] |
| Subject Public Key Info | | RSA 2048 bits |

### 7.1.6.2 Extensions

| Fields | | Criticism | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | [RFC 5280] method [0] : public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | | Yes, it is. | non-repudiation |
| **Basic Constraint** | Certificate Authority | No | False |

[9] This URL is given for information only. The authentic URL is the one in the Certificate.

[10] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime:* represents the time of request of the Certificate;
- *DocRef:* represents the identification of the document to be signed (in case of multi-signature, it is the first document that is referenced in the signature request that appears);
- *ClientId*: represents the unique identification of the client.

*The ReqTime* value is used to protect against a case of co-signatures by two (2) people with the same name. The concatenation of the three (3) information guarantees a unique value among all users.

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

| Fields | | Criticism | Value |
|---|---|---|---|
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3.1 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | https://www.mediacert.com |
| **CRL Distribution Points** | | No | http://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/crl [12] |
| **Authority Information Access** | ocsp | No | http://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/ocsp [10] |
| | caIssuers | | http://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/certificate [10] |

### 7.1.7 Organization Certificate

#### 7.1.7.1 Base fields

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the issuing Technical CA |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **Validity** | | 3 years |
| **Subject** | C | Country of the Organization |
| | OI [13] | Identifier of the Organization trained in such a way: ICD [space] Organization identifier |
| | SN [14] | Name of the authorized individual in the Organization |
| | GN [12] | First name of the individual authorized in the Organization |
| | OR [12] | Name of the unit in the Organization |
| | O | Subscriber's name |
| | SERIALNUMBER [15] | Unique DN serial number |
| | CN | Identity of the Organization |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.1.7.2 Extensions

| Fields | Criticism | Value |
|---|---|---|
| **Authority Key Identifier** | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | No | [RFC 5280] method [1]: public key identifier |

[12] This URL is given for information only. The authentic URL is the one in the Certificate.
[13] The ICD *(International Code Designator*) is on a unique 4-character code and the Organization ID is on a maximum of 35 characters.
For Organizations under French law, the ICD is 0002 and the accepted Organization ID is the Siren number.
[14] At least one of the two pieces of information must be present in the DN: the name of the unit in the Organization or the full name of the individual authorized to represent the Organization.
[15] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:

SERIALNUMBER = *CreationDate*

- *CreationDate:* represents the (arbitrary) date and time at the time of withdrawal of the Certificate: in the format *yyyyyymmddhhhmmss.*

*The CreationDate* value is used to protect against a case of co-signatures by two (2) people with the same name. The concatenation of the two (2) information guarantees a unique value among all users.

| Fields | | Criticism | Value |
|---|---|---|---|
| | | | contained in the Certificate |
| **Key Usage** | | Yes, it is. | nonRepudiation |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3.2 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | https://www.mediacert.com |
| **Subject Alternative Name** | | No | [RFC 822] : e-mail of the Certificate Holder |
| **CRL Distribution Points** | | No | http://pki-org-ac[SERIALNUMBER TCA issuer].mediacert.com/crl [16 ] |
| **Authority Information Access** | ocsp | No | http://pki-org-ac[SERIALNUMBER TCA issuer].mediacert.com/ocsp[14] |
| | caIssuers | | http://pki-org-ac[SERIALNUMBER TCA issuer].mediacert.com/certificate [14] |

[16] This URL is given for information only. The authentic URL is the one in the Certificate.

### 7.1.8 Single-use "standard" test Certificate

#### 7.1.8.1 Base fields

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the issuing Technical CA |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **Validity** | | 15 minutes |
| **Subject** | C | Nationality of the Holder |
| | SN | Name of the Holder |
| | GN | First name of the Holder |
| | OU | Subscriber's name |
| | SERIALNUMBER [17] | Unique DN serial number |
| | CN | Identity of the test holder trained in such a way:<br>TEST [space] First name of the Holder [space] Last name of the Holder [space] [TraceID] [18] |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.1.8.2 Extensions

| Fields | | Criticism | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | | Yes, it is. | nonRepudiation |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3.6 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | https://www.mediacert.com |
| **CRL Distribution Points** | | No | http://pki-otu-lcp-ac[SERIALNUMBER TCA issuer].mediacert.com/crl [19 ] |
| **Authority Information Access** | ocsp | No | http://pki-otu-lcp-ac[SERIALNUMBER TCA issuer].mediacert.com/ocsp [18] |
| | caIssuers | | https://pki-otu-lcp-ac[TCA issuer].mediacert.com/certificate [18] |

[17] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime:* represents the time of request of the Certificate;
- *DocRef:* represents the identification of the document to be signed (in case of multi-signature, it is the first document that is referenced in the signature request that appears);
- *ClientId*: represents the unique identification of the client.

*The ReqTime* value is used to protect against a case of co-signatures by two (2) people with the same name. The concatenation of the three (3) information guarantees a unique value among all users.

[18] Represents the unique identification of the trace container for the signature.

[19] This URL is given for information only. The authentic URL is the one in the Certificate.

### 7.1.9 Single-use "reinforced" test Certificate

#### 7.1.9.1 Base fields

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the issuing Technical CA |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **Validity** | | 15 minutes |
| **Subject** | C | Nationality of the Holder |
| | SN | Name of the Holder |
| | GN | First name of the Holder |
| | OU | Subscriber's name |
| | SERIALNUMBER [20] | Unique DN serial number |
| | CN | Identity of the test holder trained in such a way:<br>TEST [space] First name of the Holder [space] Last name of the Holder [space] [TraceID] [21] |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.1.9.2 Extensions

| Fields | | Criticism | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | | Yes, it is. | nonRepudiation |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3.3 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | https://www.mediacert.com |
| **CRL Distribution Points** | | No | http://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/crl [22 ] |
| **Authority Information Access** | ocsp | No | http://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/ocsp [21] |
| | caIssuers | | https://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/certificate [21] |

[20] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime:* represents the time of request of the Certificate;
- *DocRef:* represents the identification of the document to be signed (in case of multi-signature, it is the first document that is referenced in the signature request that appears);
- *ClientId*: represents the unique identification of the client.

*The ReqTime* value is used to protect against a case of co-signatures by two (2) people with the same name. The concatenation of the three (3) information guarantees a unique value among all users.

[21] Represents the unique identification of the trace container for the signature.

[22] This URL is given for information only. The authentic URL is the one in the Certificate.

### 7.1.10 Test Organization Certificate

#### 7.1.10.1 Base fields

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the issuing Technical CA |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **Validity** | | 3 years |
| **Subject** | C | Country of the Organization |
| | OI [23] | Identifier of the Organization trained in such a way: ICD [space] Organization identifier |
| | SN [24] | Name of the authorized individual in the Organization |
| | GN [22] | First name of the individual authorized in the Organization |
| | OU [22] | Name of the unit in the Organization |
| | O | Subscriber's identity |
| | SERIALNUMBER [25] | Unique DN serial number |
| | CN | TEST Organizational identity [26] |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.1.10.2 Extensions

| Fields | | Criticism | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | | Yes, it is. | nonRepudiation |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3.4 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | https://www.mediacert.com |
| **Subject Alternative Name** | | No | [RFC 822]: e-mail of the Certificate Holder |
| **CRL Distribution Points** | | No | http://pki-org-ac[SERIALNUMBER TCA issuer].mediacert.com/crl [27 ] |
| **Authority Information** | ocsp | No | http://pki-org-ac[SERIALNUMBER TCA issuer].mediacert.com/ocsp[26] |

[23] The ICD *(International Code Designator*) is on a unique 4-character code and the Organization ID is on a maximum of 35 characters.
For Organizations under French law, the ICD is 0002 and the accepted Organization ID is the SIREN number.
[24] At least one of the two pieces of information must be present in the DN: the name of the unit in the Organization or the full name of the individual authorized to represent the Organization.
[25] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:

SERIALNUMBER = *CreationDate*

- *CreationDate:* represents the (arbitrary) date and time at the time of withdrawal of the Certificate: in the format *yyyyyymmddhhhmmss.*

*The CreationDate* value is used to protect against a case of co-signatures by two (2) people with the same name. The concatenation of the two (2) information guarantees a unique value among all users.
[26] The word "TEST" and the identity of the Organization are not separated by a space.
[27] This URL is given for information only. The authentic URL is the one in the Certificate.

| Fields | | Criticism | Value |
|---|---|---|---|
| **Access** | caIssuers | | http://pki-org-ac[SERIALNUMBER TA issuer].mediacert.com/certificate[26] |

## 7.2 CRL Profile

### 7.2.1 Base field

| Fields | | Value |
|---|---|---|
| **Version** | | 1 (for version 2) |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **This Update** | | Date of issue of the CRL |
| **Next Update** | | Date of issue of the CRL + 7 days [28] |
| **Revoked Certificates** | userCertificate | Unique serial number of the revoked Certificate |
| | revocationDate | Date of revocation |
| | crlEntryExtensions | Additional information that can be provided in CRL input extensions |

### 7.2.2 Extensions

| Fields | Criticism | Value |
|---|---|---|
| **Authority Key Identifier** | No | [RFC 5280] method [0]: identifier of the public key of the sending TCA |
| **CRL Number** | No | CRL number defined by the issuing Technical CA |

### 7.2.3 Input extensions

| Fields | Criticism | Value |
|---|---|---|
| **Reason Code** | No | [RFC 5280]: code corresponding to the correct revocation reason |

[28] In the case of the termination of the CA, the last published CRL shall be valid for three (3) years or more.

## 7.3 OCSP Profile

In accordance with chapter 4.10 this document, MediaCert TSP provides users with an OCSP responder so that they can check the real-time status of Certificates issued by CAs online. This service complies with [RFC 6960].

### 7.3.1 OTU CA

In this context, the OCSP answering machine has a Certificate issued by the OTU CA, the profile of which is detailed below.

#### 7.3.1.1 Base field

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the issuing Technical CA |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **Validity** | | 3 years |
| **Subject** | C | FR |
| | OI | 0002 378901946 |
| | OU | AC OTU |
| | O | Worldline |
| | SERIALNUMBER [29] | Unique DN serial number |
| | CN | Service OCSP PKI OTU |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.3.1.2 Extensions

| Fields | | Criticism | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | | Yes, it is. | Digital Signature |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualify | | https://www.mediacert.com |
| **Extended Key Usage** | | No | ocspSigning (1.3.6.1.5.5.7.3.9) |
| **CRL Distribution Points** | | No | http://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/crl [30] |
| **Authority Information Access** | ocsp | No | http://pki-otu-ac[SERIALNUMBER TCA issuer].mediacert.com/ocsp [29] |
| | caIssuers | | http://pki-otu-ac[SERIALNUMBER TCA |

[29] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:
SERIALNUMBER = incremented number each time an OCSP certificate is issued for the issuing Technical CA in question.
[30] This URL is given for information only. The authentic URL is the one in the Certificate.

| Fields | | Criticism | Value |
|---|---|---|---|
| | | | issuer].mediacert.com/certificate [29] |

### 7.3.2 OTU LCP CA

In this context, the OCSP responder has a Certificate issued by the OTU LCP CA and whose profile is detailed below.

#### 7.3.2.1 Base field

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the issuing Technical CA |
| **Signature** | | sha256WithRSAEncryption (1.2.2.840.113549.1.1.1.11) |
| **Issuer** | | DN of the issuing Technical CA |
| **Validity** | | 3 years |
| **Subject** | C | FR |
| | IO | 0002 378901946 |
| | OU | AC OTU LCP |
| | O | Worldline |
| | SERIALNUMBER [31] | Unique DN serial number |
| | CN | Service OCSP PKI OTU LCP |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.3.2.2 Extensions

| Fields | | Criticism | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | [RFC 5280] method [0]: public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | [RFC 5280] method [1]: public key identifier contained in the Certificate |
| **Key Usage** | | Yes, it is. | Digital Signature |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentify | No | 1.2.250.1.111.20.5.3 |
| | policyQualifyId | | 1.3.6.1.5.5.7.2.1 |
| | qualify | | https://www.mediacert.com |
| **Extended Key Usage** | | No | ocspSigning (1.3.6.1.5.5.7.3.9) |
| **CRL Distribution Points** | | No | http://pki-otu-lcp-ac[SERIALNUMBER ACT issuer].mediacert.com/crl [32] |
| **Authority Information Access** | ocsp | No | http://pki-otu-lcp -ac[SERIALNUMBER ACT issuer].mediacert.com/ocsp [31] |
| | caIssuers | | http://pki-otu-lcp -ac[SERIALNUMBER ACT issuer].mediacert.com/certificate [31] |

[31] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:
SERIALNUMBER = incremented number each time an OCSP certificate is issued for the issuing Technical CA in question.
[32] This URL is given for information only. The authentic URL is the one in the Certificate.

### 7.3.3 ORG CA

In this context, the OCSP answering machine has a Certificate issued by the CA ORG and whose profile is detailed below.

#### 7.3.3.1 Base fields

| Fields | | Value |
|---|---|---|
| **Version** | | 2 (for version 3) |
| **Serial number** | | Defined by the CA Transmitting Technique |
| **Signature** | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| **Issuer** | | DN of the sending ACT |
| **Validity** | | 3 years old |
| **Subject** | C | FR |
| | OI | 0002 378901946 |
| | OU | AC ORG |
| | O | Worldline |
| | SERIALNUMBER [33] | Unique serial number of DN |
| | CN | OCSP PKI ORG Service |
| **Subject Public Key Info** | | RSA 2048 bits |

#### 7.3.3.2 Extensions

| Fields | | Critical | Value |
|---|---|---|---|
| **Authority Key Identifier** | | No | RFC 5280] method[0] : public key identifier of the issuing CA |
| **Subject Key Identifier** | | No | RFC 5280] method[1] : public key identifier contained in the Certificate |
| **Key Usage** | | Yes | Digital Signature |
| **Basic Constraint** | Certificate Authority | No | False |
| **Certificate Policies** | policyIdentifier | No | 1.2.250.1.111.20.5.3 |
| | policyQualifierId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | https://www.mediacert.com |
| **Extended Key Usage** | | No | ocspSigning (1.3.6.1.5.5.7.3.9) |
| **CRL Distribution Points** | | No | http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [34] |
| **Authority Information Access** | ocsp | No | http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [34] |
| | caIssuers | | http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [34] |

[33] According to [RFC 3739], the SERIALNUMBER field is used to remove the risk of homonymy in the remaining fields of the DN. It is built as follows:
SERIALNUMBER = incremented number each time an OCSP certificate is issued for the issuing Technical CA in question.

[34] This URL is given for information only. The authentic URL is the one in the Certificate.

# 8 Compliance audit and other evaluations

## 8.1 Frequency and/or circumstances of evaluations

Worldline, as part of the evaluation of this certification service, conducts an external certification audit to the [ETSI 319 411-1] standard of PKI submitted within this CP-CPS every two (2) years by an accredited organization.

In addition, Worldline carries out a surveillance audit (internal or external) between two (2) external audits of Certification to the standard [ETSI 319 411-1].

## 8.2 Identities / qualifications of assessors

All requirements and practices described in the [GP] apply.

## 8.3 Relations between evaluators and evaluated entities

All requirements and practices described in the [GP] apply.

## 8.4 Topics covered by the evaluations

All requirements and practices described in the [GP] apply.

## 8.5 Actions taken in response to evaluation findings

All requirements and practices described in the [GP] apply.

## 8.6 Communication of results

All requirements and practices described in the [GP] apply.

# 9 Other business and legal issues

## 9.1 Tariffs

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

### 9.1.1 Fees for the provision or renewal of a Certificate

This is dealt with in the context of the higher level service agreement between Worldline and the Subscriber.

### 9.1.2 Fees for accessing Certificates

This is dealt with in the context of the higher level service agreement between Worldline and the Subscriber.

### 9.1.3 Rates for accessing status and revocation information on Certificates

Not applicable.

### 9.1.4 Rates for other services

Not applicable.

### 9.1.5 Refund policy

Not applicable.

## 9.2 Insurance

### 9.2.1 Insurance coverage

All requirements and practices described in the [GP] apply.

### 9.2.2 Other resources

All requirements and practices described in the [GP] apply.

### 9.2.3 Coverage and guarantee for user entities

Not applicable.

## 9.3 Confidentiality of professional data

### 9.3.1 Scope of confidential information

All requirements and practices described in the [GP] apply.

In particular, within the scope of this CP-CPS, the following information is considered confidential:

- the TDCP;
- CA private keys;
- activation data associated with CA private keys;
- all the secrets of the PKI;
- event logs of the PKI components;
- the registration files of the holders;
- audit reports.

### 9.3.2 Information outside the scope of confidential information

All requirements and practices described in the [GP] apply.

### 9.3.3 Responsibilities in terms of protecting confidential information

All requirements and practices described in the [GP] apply.

The specific additional requirements and practices defined below also apply.

#### 9.3.3.1 Applicable legislation

Law n° 2018-493 of 20 June 2018, promulgated on 21 June 2018, amended the Data Protection Act in order to bring national law into line with the European legal framework.
Worldline processes personal data in accordance with the French legislation in force on French territory, which complies with that prevailing on European territory, with regard to the protection of personal data. Worldline takes all appropriate and necessary measures in accordance with these regulations to ensure that the personal data it is required to store via the PKIs are protected from any compromise, breach of security or loss of integrity that could have an impact on the trust service provided and the personal data stored therein.

To this end, the MediaCert TSP implements security measures for premises and information systems to prevent the files held from being distorted, damaged or accessed by unauthorized third parties.

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

When creating registration files, a set of personal data is required. They are transmitted to the Registration Authority by Subscribers or their representative.

##### [OTU CA][OTU LCP CA] Single-use Certificates

In the context of Single-use Certificates, it is recalled that the Subscriber shall ensure that he/she obtains the express consent of the future Holders to the processing and storage of their data by

the PKI, before transmitting their personal data, for the processing of requests to create this type of Certificate.
To this end, the future Holder must accept before any request initiated on its behalf by the Subscriber that the personal data concerning it, transmitted by the Subscriber to the Registration Authority, be processed electronically for the sole purpose of:

- constitute its identification and allow its authentication in order to generate a Certificate in its name;
- be able to provide him the activation data of his private key;
- make it possible to support the identity indicated in the Certificate by providing the necessary proof, if necessary, by keeping the elements in the registration file.

In addition, such supporting documents may, where appropriate, be subject to an automated check to verify the consistency of the fields. In the event of unsuccessful or negative controls, manual controls will be carried out by the Organization with which the Holder is in contact.

The consent of the future Data Controller for these processing operations, in the context of the implementation of the electronic signature, must be expressed by means of positive action on his part, the latter must be informed in advance of the consequences of his choice and be able to have the means to exercise it.

In this respect, it is specified that any opposition to the retention of personal data will prevent the issuance of this type of Certificate. Indeed, by accepting the provision of the Certificate to proceed with an electronic signature, the Holder accepts that the CA retains, via the RA and at the request of the RA, the personal data for the duration necessary to fulfil the purposes of the processing operations carried out in the context of the provision and management of the Single-use Certificate. Indeed, the PKI must be able to meet the obligations to which it is subject in the context of the audits it is required to pass, justify compliance with the chosen level or levels of certification, the identification functions assigned to the electronic signature, the rules of the art and the applicable standards.

The Subscriber shall ensure that the Holder is fully informed and that the designated service provider complies with the applicable legal provisions on the protection of personal data.

### [ORG CA] Organization Certificates

As part of the preparation of the registration file, the Subscriber, via his representatives, provides the Registration Authority with a set of personal data necessary for the preparation of the file. This transmission by the Subscriber's representative is made in knowledge of the purposes attached to this collection. To this end, the Subscriber's representatives and any representatives of the Organization must agree that the personal data concerning them may be processed electronically for the sole purpose of:

- constitute their identification and, in the case where the Subscriber and the Organization are the same entity, allow their authentication, in order to generate a Certificate containing their information;
- make it possible to support the identity, if any, given in the Certificate and the powers conferred by providing the necessary evidence, if necessary, by keeping the elements in the evidence file.

Consequently, by agreeing to represent the Subscriber, the Subscriber's representatives will have previously agreed that their personal data may be processed and stored for as long as required

for the purposes of the processing operations carried out in the context of the provision and management of Organization Certificates.

#### 9.3.3.3 Data subject's rights to data

In accordance with Article 39 of the Data Protection Act, amended by Act No. 2018-493 of 20 June 2018, and Article 14 of the GDPR, any natural person who can prove his identity has the right to request access to his personal data under the conditions referred to in these articles.

Any natural person proving his identity may request the rectification, updating or deletion of his personal data.
In the case of Single-use Certificates, the personal data used to support the identification of the Holder for the production of the Certificate with which he/she has signed may only be rectified, locked or deleted once the purpose for which the said personal data were collected and the processing has been completed.
The same applies to personal data collected for the issuance of Organization Certificates.
The personal data used to identify and authenticate the future Certificate holder communicated during the electronic signature process or the constitution of the registration file remain in the history of the traces of the transaction and the electronic signature performed until the purpose for which the personal data were collected and the processing carried out has been completed.
The same applies to the personal data provided when requesting the creation of an Organization Certificate.

As a result of the foregoing provisions, persons who have given their prior consent to the processing of their personal data by the PKI as set out in this document may, in accordance with the law, access and obtain a copy of all information concerning them held by the PKI.

None of the personal data communicated when registering the Holder or when preparing the registration file for Subscribers and Organizations may be used by the PKI for any purpose other than that defined under the CP-CPS.

The right of access may be exercised in writing: by post to the MediaCert TSP contact point, at the address given in chapter 1.6.2 this document or on the MediaCert TSP website (see chapter 2.2), accompanied by a copy of an identity document. Ideally, by registered mail with acknowledgement of receipt.

#### 9.3.3.4 Conditions for disclosing personal information to judicial or administrative authorities

Worldline may have to make the registration records of Registrants, Subscribers and Organizations available to authorized third parties in legal proceedings or audits to verify the issuance of Certificates. The PKI has secure procedures to allow this access, which are tracked by name and stored.

## 9.4 Protection of personal data

### 9.4.1 Personal data protection policy

All requirements and practices described in the [GP] apply.

To this end, the Registration Authority collects and processes the identification data of future Registrants, Subscribers or representatives contacts, Organizations or representatives contacts contained in the registration files (evidence file).

### 9.4.2 Personal information

The registration data of the Registrant or Authorized Individuals as provided by the Subscriber is information considered personal. Access to personal data shall be provided in accordance with the [GP].

### 9.4.3 Non-personal information

Not applicable.

### 9.4.4 Responsibility for the protection of personal data

All requirements and practices described in the [GP] apply.

### 9.4.5 Notification and consent to the use of personal data

In accordance with the laws and regulations in force in France, personal information provided by holders to the PKI is not disclosed or transferred to a third party except in the following cases: prior consent of the holder, judicial decision or other legal authorization.

### 9.4.6 Conditions for disclosing personal information to judicial or administrative authorities

All requirements and practices described in the [GP] apply.

### 9.4.7 Other circumstances for disclosing personal information

Not applicable.

## 9.5 Intellectual and industrial property rights

All requirements and practices described in the [GP] apply.

## 9.6 Contractual interpretations and guarantees

The obligations common to the components of the PKI are as follows:

- protect and guarantee the integrity and confidentiality of their secret and/or private keys;
- use their cryptographic keys (public, private and/or secret) only for the purposes intended when they are issued and with the tools specified under the conditions set out in the CA CP-CPS and related documents (see chapter 1.5);
- respect and apply the part of the [TDCP] for which they are responsible (this part must be communicated to the corresponding component);
- submit to compliance checks carried out by the audit team mandated by the CA (see chapter 7.3.3);
- respect the agreements or contracts that bind them between themselves or to the holders;

- document their internal operating procedures, implement the resources (technical and human) necessary to carry out the services to which they commit themselves under conditions guaranteeing quality and safety;
- have non-discriminatory practices in their policies and procedures.

### 9.6.1 Certification Authority

The obligation of the CAs is to:

- ensure that the Registration Authority acting on behalf of the OTU CA complies with this CP-CPS;
- publish the public information referred to in chapter 2.2 this document, in particular the General Terms and Conditions of Subscription [GCSubscription] and the General Terms and Conditions of Services [GCServices], in a sustainable and secure manner;
- make its services accessible to any Subscriber who has accepted the General Terms and Conditions of Subscription [GCSubscription];
- collaborate with auditors during compliance checks and implement any measures decided with auditors following compliance checks.

### 9.6.2 Registration service

The obligation of RA is to:

- comply with the registration procedures described in this CP-CPS.

### 9.6.3 Certificate Holders

The beneficiaries of Certificates are required to:

- protect the means of access to private keys and Certificates;
- use their Certificates only for the uses intended and defined in the associated CP-CPS;
- revoke or request the revocation of their Certificate in the event of compromise or suspected compromise;
- revoke or request the revocation of their Certificate in the event of compromise or suspicion of compromise of the above-mentioned means of access;
- verify and comply with the obligations incumbent on them described in this document and in the General Terms and Conditions of Services [GCServices].

#### 9.6.3.1 Subscriber

In addition to the obligations defined in chapter 9.6.3 Subscriber has different obligations depending on the type of Certificate, which is shown below.

### [OTU CA][OTU LCP CA] Single-use Certificates

For a Single-use Certificate, the Online CA Subscriber is required to:

- collect and verify or have collected and have verified under its responsibility the identity information provided by the future Holder;
- communicate to the Holder his obligations (see chapter 9.6.3.2);
- inform the Holder of the Certificate application process and the consequences of its use in this CP-CPS;
- transmit, in its request, the data relating to the identification of the future Holder as well as all the necessary consents of this future Holder as defined in chapter 3.2.3.1 this document;
- constitute and sign the application for the Certificate of the future Holder;
- keep exclusive control of its authentication resources with the Registration Authority;
- communicate as soon as possible to the Registration Authority any event that may affect the quality of the identification of its future Registrants;
- communicate as soon as possible to the Registration Authority any event that may affect the reliability of its means of authentication with the latter;
- to engage in non-discriminatory practices.

### [ORG CA] Organization Certificates

For an Organization Certificate, the Subscriber to the CA is required to:

- complete the Certificate creation request file by providing all the required elements, supporting documents and necessary powers (see chapter 4.1.2.2). The information and supporting documents communicated to the Registration Authority must be accurate, sincere and up to date when requesting the creation of a Certificate;
- inform the Registration Authority in the event that the data in the Certificate is no longer valid due to a change within the Organization. In this respect, the Subscriber must notify the RA without delay, by registered letter with acknowledgement of receipt:
    - any change in the identity of the person acting as Subscriber's representative or Deputy Subscriber's representative, as well as the effective date of such change, together with supporting documents;
    - any changes in the information provided to RA, as well as the effective date of these changes.
- request revocation of the Certificate in the cases listed in this document. In this respect, the modification of information contained in the Certificate of Organization entails the revocation of the Certificate and its replacement at the Organization's expense;
- communicate as soon as possible to the Registration Authority any event that may affect the reliability of the means of authentication with the latter. In this respect, changes (first name, surname, e-mail address) must be notified to the RA;

- inform the Registration Authority if the Organization no longer exists. In this respect, the Subscriber must notify the RA without delay, by registered letter with acknowledgement of receipt, of any changes (first name, surname, e-mail address, Organization ID) affecting all the Organization's Certificates, accompanied by supporting documents;

- inform the Registration Authority in the event that information concerning the Organization, not included in the Certificate of Organization and having no impact on its validity, is modified. In this respect, the Subscriber must notify the RA as soon as possible, by simple letter, of changes in information;

- to engage in non-discriminatory practices.

In the event that the Subscriber uses a technical service provider, it is his responsibility to ensure that the latter complies with these obligations, especially since this service provider may hold secrets specific to the Subscriber: private keys corresponding to authentication and message signature Certificates. It is therefore the Subscriber's responsibility to ensure that measures to protect access to these secrets are properly implemented.

#### 9.6.3.2 Holders

In addition to the obligations defined in chapter 9.6.3 future holder has the duty to provide information and supporting documents, requested by the Subscriber, which he certifies as accurate and up to date when applying for the Certificate.

The obligations of the future Holder are also defined in the contract concluded with his representative, here referred to as the Subscriber.

### 9.6.4 Certificate Users

Users of Certificates must:

- verify and comply with the obligations incumbent on them in this document and in the General Terms and Conditions of Services [GCServices]. These obligations will be for the Single-use Certificates described by the Subscriber in the contract binding him to the future Holder (see chapter 9.6.3.1). This contract sets out the operation of a signature in electronic form, the implications of this choice, the procedures for carrying it out with the necessary consents in accordance with those set out in its Subscription Contract;

- verify and respect the use for which a Certificate has been issued;

- for each Certificate in the Certification Chain, from the Subscriber's Certificate to the Root CA, verify the digital signature of the CA issuing the relevant Certificate and check the validity of this Certificate (validity dates, revocation status).

### 9.6.5 Other participants

Not applicable.

## 9.7 Limit of guarantee

Online CAs undertake to issue Certificates in accordance with this document, as well as with the state of the art and technology.

MediaCert TSP guarantees through its services:

- the Subscriber's authentication with his Certificate by the Registration Authority;
- the generation of Certificate(s) in accordance with the Subscriber's request, previously authenticated and verified;
- the provision of information functions on the status of Certificates issued, following the Subscriber's request, by CAs in accordance with this document;
- the exclusive control of the private key of the Certificate by the Certificate Carrier Device and the destruction of the same key after a single session of use in the case of a Single-use Certificate.

No other guarantees are provided.

## 9.8 Limitation of liability

MediaCert TSP can only be held liable in the event of proven non-compliance with its obligations.

The MediaCert TSP may not be held liable in the event of a fault in the scope of a Subscriber entity, in particular in the event of:

- use of an expired Certificate;
- use of a revoked Certificate;
- use of a Certificate in an application other than those described in chapter 4.5 this CP-CPS.

MediaCert TSP is generally not responsible for the documents and information provided by the Subscriber and does not guarantee their accuracy or the consequences of harmful facts, actions, negligence or omissions of the Subscriber, his representative or the Holder.

The Subscriber undertakes not to make any commitment in the name and on behalf of the MediaCert TSP, which it may under no circumstances replace.

## 9.9 Indemnities

The issuance of Certificates by the CAs concerned by this document is carried out as part of higher level services such as electronic subscription.

The master agreement signed between the customer and Worldline, or its duly authorized agent, specifies the conditions for compensation in the event of damage. In the absence of a master agreement, Worldline's General Terms and Conditions of Sale will apply.

## 9.10 Duration and early termination of the validity of the CP

### 9.10.1 Period of validity

The CP-CPS is made effective once validated by the entity responsible for this document (see chapter 1.6.1). It must remain in force at least until the end of the life of the last Certificate issued under this CP-CPS.

### 9.10.2 Early termination

This CP-CPS remains in use until a new version is released.

### 9.10.3 Effects of the end of validity and remaining clauses applicable

Despite the replacement of this CP-CPS by a new version, the last Certificates issued when it was still valid shall apply this document to the said Certificates and to the various actors until the expiry of the Certificates in question.

## 9.11 Individual notifications and communications between participants

MediaCert TSP will inform its Subscribers by e-mail no later than one (1) month before the publication of the new version of this document, in the event of any change affecting this CP-CPS.

The Subscriber will also be informed of the effective implementation of the new version of the CP-CPS no later than one (1) month following its publication via a signed e-mail communiqué.
In addition, the Subscriber will be informed of any changes to the General Terms and Conditions of Subscription, the General Terms and Conditions of Services or the General Terms and Conditions of Sales via an e-mail message.

All components and actors of the CAs are kept informed, through an internal communiqué, of the amendments made to this document and the possible impacts that may result from them.

No requirement for Subscribers to validate changes is made in this document. Indeed, the use of the services after notification of the changes made implies automatic acceptance of these changes.

## 9.12 Amendments to the CP

### 9.12.1 Amendment procedures

All requirements and practices described in the [GP] apply.

### 9.12.2 Mechanism and information period for amendments

In the event of a change that requires the modification of this CP-CPS, information on the mechanism and information period for amendments is provided in chapter 9.11.

### 9.12.3 Circumstances under which the OID must be changed

All requirements and practices described in the [GP] apply.

## 9.13 Provisions concerning conflict resolution

All requirements and practices described in the [GP] apply.

The master agreement signed between the Subscriber and Worldline, or its duly authorized representative, specifies the provisions concerning dispute resolution. In the absence of a master agreement, Worldline's General Terms and Conditions of Sale will apply.

The authorized contact for any comments, requests for additional information, complaints or dispute files concerning this CP-CPS is defined in chapter 1.6.2. All requests must be made by e-mail with acknowledgement of receipt or by registered post with acknowledgement of receipt.

## 9.14 Competent Jurisdictions

All requirements and practices described in the [GP] apply.

The master agreement signed between the client and Worldline, or its duly authorized representative, specifies this provision. In the absence of a master agreement, Worldline's General Terms and Conditions of Sale will apply.

## 9.15 Compliance with laws and regulations

All requirements and practices described in the [GP] apply.

## 9.16 Miscellaneous provisions

### 9.16.1 Global agreement

Not applicable.

### 9.16.2 Transfer of activities

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

All requirements and practices described in the [GP] apply.

The master agreement signed between the client and Worldline, or its duly authorized representative, specifies this provision. In the absence of a master agreement, Worldline's General Terms and Conditions of Sale will apply.

## 9.17 Other provisions

### 9.17.1 Independence of the parties and non-discrimination

All requirements and practices described in the [GP] apply.

### 9.17.2 Risk analysis

All requirements and practices described in the [GP] apply.

### 9.17.3 Contractual documents

In the event of any contradiction between the articles of the General Terms and Conditions of Subscription [GCSubscription] and those of the provisions of the Higher Level Service Agreement (Framework Agreement), the clauses of the General Terms and Conditions of Subscription [GCSubscription] which are based on the applicable Certification Policy - Declaration of Certification Practices shall prevail.