Document reference:	OTU.PC.0002
Document revision:	2.0
Document date:	07/11/2016
Classification:	PUBLIC

OTU Certification Authority

Certification Policy

www.worldline.com

Contents

Change log

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 • added procedures and reasons for destroying CA key pairs in subsection 6.3.4; • the word "operator" has been replaced by "pilot"; • made guarantee limitations consistent with the General Terms of Use (section 9.7); • modified paragraph 4.9.3.2 to describe the procedure for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

			• added the methods that guarantee that the revocation period is complied with (paragraph 4.9.3.2 and subsection 5.7.3); • added subsections 5.2.5 and 5.2.6, and modified subsection 5.3.6 so the CA complies with the requirements set out in subsection 7.4.3; • added subsection 5.4.6 about the procedures for returning and verifying the return of event logs; • modified subsection 5.2.4 about the roles requiring remit separation; • added the OIDs of test certificates (subsection 1.2.2); added descriptions (paragraphs 7.1.2.4 and 7.1.2.5); • added the OTU CP's OID into all certificate templates; • added paragraph 4.9.10 about CRL archiving; • added description of the monitoring of the Mediacert page (subsection 2.4.2); • added a reference to the signing of the CA's documents to make sure they have been authenticated (subsection 2.4.3) ; • revised subsection 5.3.2 about the verification of criminal records; • modified templates and OIDs to keep up with the change of version of the CP (subsection 1.2.2, and paragraphs 7.1.2.2, 7.1.2.3, 7.1.2.4 and 7.1.2.5); • added a sentence to subsection 3.2.4 to indicate that the e-mail address is not verified during the certificate request; • corrected subsection 7.1.5 about the name constraints that affect the CN attribute, and the GN and SN attributes in the case of Organisation certificates; • modified subsection 9.12.2 about the circumstances under which the OID must be changed; • added missing definitions; • rewording and clarifications on the contract, the subscription file, the Subscriber's obligations, Subject identification and Organisation validation; • added a step of acceptance of the Certificate by the Subject of an OTU certificate; and • added to section 9.6 a pledge against discriminatory practices.

1. Introduction

1.1 Purpose of the document

This document describes the certification policy (CP) of the **OTU CA** that has been created to govern the creation, issuance and life cycle of

- the OTU signing certificates implemented as part of the OTU online subscription service; and
- the server certificates or electronic certificates used to seal electronic data, thus guaranteeing their origin and integrity.

In this context, this CP describes:

- the requirements which the **OTU CA** abides when registering and verifying certificate requests,
- the management of certificates throughout their life cycles,
- the security measures applicable to the key management infrastructure,
- the uses for which these certificates are issued, and
- the obligations and requirements of the various participants.

This CP is applicable to the certificates intended a certificate Holder mechanism managed by Worldline.

This CP is completed by a second document called **Certification Practice Statement** [CPS], which sets out the certificate management practices of a CA. This document describes how the **OTU CA** is implemented:

- IT and network resources;
- external software packages and proprietary services;
- physical security implemented on hosting sites;
- logical security of IT resources;
- certificate management procedures; and
- operation and staff training procedures.

Therefore, the CPS is the answer to the requirements specified in the CP.

1.2 Identification

1.2.1 Document identification

Elements	Value
Title	Certification Policy of the OTU Certification Authority
Document reference	OTU.PC.0002
Version	2.0
Author	Worldline
Product reference	OTU Certification Authority
Keywords	Certification Authority, Certification Policy, CP, Electronic certification, Electronic signature

1.2.2 Certification Authority identification

The Certification Authority is called "**OTU**".

AFNOR (*the French national organisation for standardisation*) has assigned number **1.2.250.1.111** to "Worldline".

OIDs are based on Worldline's OID and built as follows: 1.2.250.1.111.x.y.z.w where:

- x is the year on which the PC was created e.g. 2012 => 12
- y is a number indicating that the document was the "y"-th document created during the year (in the CP number specified below, y=7 means that the CP was the seventh document created in 2012.).
- z is the version of the CP.
- w is the type of certificate within the CA.

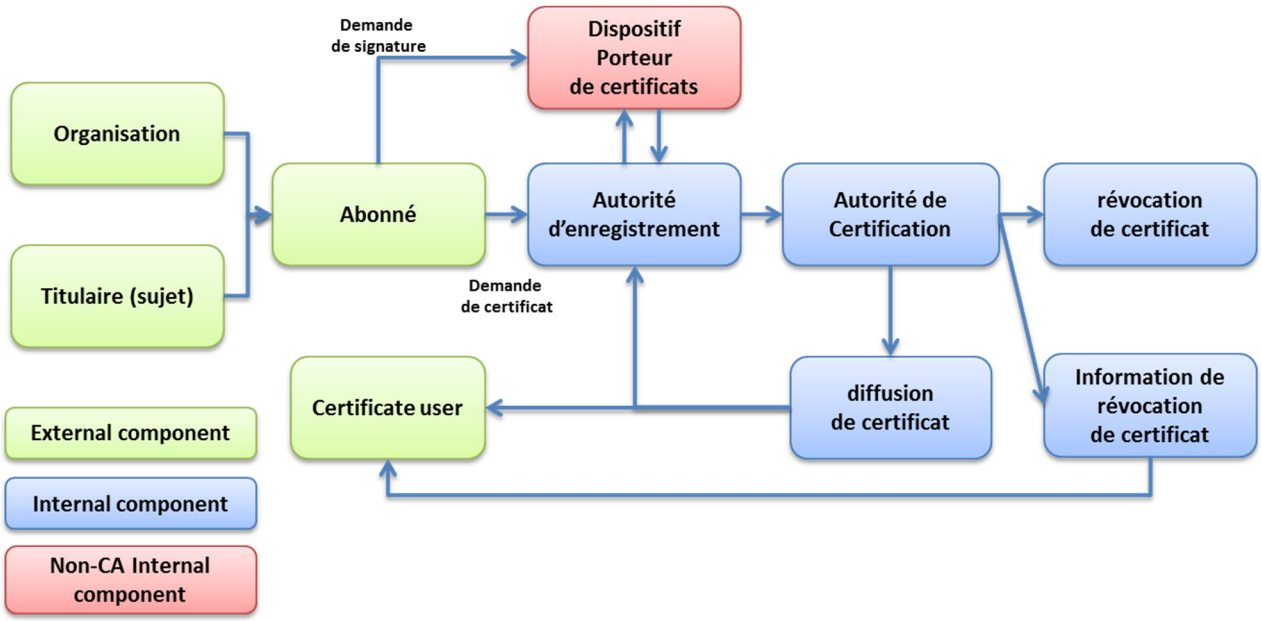
The OID of the **OTU CA**'s CP is **1.2.250.1.111.12.7.2**

- One-time-use certificate OID: 1.2.250.1.111.12.7.2.1
- Organisation certificate OID: 1.2.250.1.111.12.7.2.2
- OID of a One-time-use Certificate for test purposes: 1.2.250.1.111.12.7.2.3
- OID of an Organisation Certificate for test purposes: 1.2.250.1.111.12.7.2.4

1.3 PKI components

1.3.1 PKI functional diagram

The OTU PKI implemented consists of several functional components that are described in detail in section 1.3.



1.3.2 CA hierarchy

The **OTU CA** is the subordinate of an Atos Worldline Root Certification Authority.

DN:

C = FR
O = Atos Worldline
OU = 0002 378901946
CN = AC Racine - Root CA - 2012

OID: 1.2.250.1.111.12.4.1

1.3.3 OTU CA certification authorities

It is imperative that the **OTU CA** implement this OTU CP.

The **OTU CA** signs the certificates that it issues with its private key and is responsible for them.

For this purpose, the **OTU CA** relies on a technical infrastructure called Public Key Infrastructure (PKI).

The services that the PKI provides are the product of various services that correspond to the various stages of the life cycles of key pairs and certificates.

Functionally, the OTU PKI can be broken down as follows:

- Registration Authority,
- Certificate Generation Service,
- Certificate Delivery Service,
- Certificate Revocation Service and
- Certification Status Information Service.

1.3.3.1 Certification Authority

Here, this term refers to the technical part of the Certification Authority or certification service. It is the entity that produces certificates at the request of the Registration authority. It is also in charge of the complete life cycle of the certificate (manufacturing, publication, etc.).

This authority generates certificates from

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

These certificates are signed electronically with the **OTU CA**'s private key.

The Certification Authority is also represented by an Authority manager appointed at Worldline.

1.3.3.2 Certificate delivery service

This function delivers the certificate signed by the Certification Authority to the Registration Authority. This certificate is then sent to the certificate Holder mechanism so it can be used within the scope described in section 1.4.

1.3.3.3 Certificate revocation service

This service processes certificate revocation requests. The processing results are given through the certificate status information service.

1.3.3.4 Certificate status information service

This function gives certificate users information about the statuses of certificates (revoked, etc.) by means of a Certificate Revocation List (CRL).

1.3.4 Registration Authority (RA)

The RA is the contact of the customer units (Subscribers) that send certificate requests to it. This is where the following operations are carried out:

- authentication of the Subscriber that makes the request,
- verification of the content of certificate requests,
- registration of certificate requests,
- certificate delivery,
- archiving of certificate requests,
- registration of revocation requests,
- acceptance or refusal of revocation requests, and
- archiving of revocation requests.

To provide these services, the RA has at its disposal the technical and human resources needed to manage the life cycles of certificates for the CA. Therefore, the RA is a single point of access to the CA (servers used to send requests and deliver certificates).

1.3.5 Certificate Holder mechanism

In the context of this CP, the certificate Holder is different from the certificate Subject.

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

The certificate Holder mechanism carries out the following tasks for each certificate generated by the CA:

- generation of the key pair;
- secure storage of the key pair;
- generation of the Certificate Signing Request (CSR) that contains the user information given by the Subscriber;
- use of the private key and the certificate to sign documents electronically
    - on behalf of the Organisation through its representative, or
    - on behalf of the certificate Subject.
- destruction of the private key (according to the types of certificates; see **Erreur ! Source du renvoi introuvable.**).

The certificate Holder mechanism stores the secret data securely and has exclusive control over them on behalf of the Subject or Organisation.

1.3.6 Subscriber and Subject

For the **OTU CA** to deliver certificates, a Subscription contract must have been signed beforehand with the OTU Certification Authority. This contract specifies the type of certificate that the Subscriber wants to implement:

- OTU signing certificate issued in the name of a natural person so documents can be signed electronically, and / or
- electronic certificates for sealing documents on behalf of its Organisation or principals (Organisations).

It must be noted that in the case of OTU CA signing certificates, the Subscriber requests certificates from the OTU Certification Authority. In this case, the Subscriber

- must, before requesting a certificate for the Subject, have identified the latter so the issued certificate can be based on a reliable, reasonably verified identity.
- must have obtained from the Subject the required consent to be able to request from the CA the generation of an OTU certificate.
- In this case, the Certification Authority will produce a one-time-use certificate (see. 1.4.1).

To seal electronic data on behalf of Organisations that are associated with the Subscriber, legally or through an agreement, the Certification Authority produces Organisation certificates (see 1.4.2).

1.3.7 Certificate user

The user is the natural or legal person that uses the information of a certificate that they receive (here through an electronic signature). This signature is associated with a digital document (PDF document).

It should be noted that the signature of a PDF document is mostly used by the products supplied by ADOBE™, such as Acrobat Reader©. These products make it possible to view the signature of the document, which is not the case of all other PDF viewers.

1.3.8 Organisation

An Organisation is associated with a Subscriber. The latter will request for the former an electronic signature certificate containing the Organisation's name. This certificate is only used as part of the PDF sealing service operated by Worldline.

Through the Subscriber, the Organisation uses a certificate operated by Worldline to store and seal documents in its stead as part of a delegation granted by the Subscriber to Worldline.

Although the Subscriber and the Organisation are the same entity in most cases, it is possible to make a difference between the two.

For instance, a Subscriber may want to use a brand name rather than the name of the company that has subscribed. Besides, if a group has multiple subsidiaries, the Subscriber and the Organisation may have different names.

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

An Organisation certificate can refer to a person who is either the legal representative appearing on the Organisation's company registration certificate, or a person who has been duly authorised to appear on the certificate for conventional or statutory reasons. In any case, the competent authorities of the Organisation must have duly authorised the person to appear as Subscriber representative or deputy Subscriber representative. In this case, this person's name appears on the Organisation certificate produced by the **OTU CA**.

In accordance with the ETSI specifications document, an Organisation must be considered as a Subject. However, this CP refers to the Organisation by name.

1.3.9 Other participants

Human resources complete the system:
- IT systems operators (who maintain the operational condition of the system), and
- teams in charge of maintaining the compliance of the system.

1.4 Types of certificates

The OTU CA produces two types of certificates. The main difference between them is their OID (see 7.1).

1.4.1 One-time-use certificate

A one-time-use certificate is produced by the Certification Authority for a natural-person Subject at the Subscriber's request.

This certificate has a very short life span and makes it possible to sign a PDF document on behalf of the Subject at the Subscriber's request.

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

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

The signature of the message is validated during the signing request.

The Subscriber is responsible for the identification data that are sent to the Registration Authority in the request and which make it possible to create a certificate that contains the Subject's verified data.

Subjects' private keys generated in a dedicated secure piece of equipment (Hardware Secure Module) that has been certified in accordance with the FIPS 140-2 specification, level 2 or higher.

Once the one-time-use certificate has been used at the Subscriber's request, the corresponding private key is destroyed in the HSM.

1.4.2 Organisation certificate

The Organisation certificate is delivered as part of the PDF sealing service that Worldline operates on its own premises on behalf of the Organisation.

The Organisation certificate enables this Organisation to request from Worldline the sealing of PDF documents by an Organisation (Certification).

The Subscriber sends the sealing request to the certificate Holder mechanism by means of a message that the Subscriber signs electronically.

Requests for such certificates are made in accordance with a procedure that involves an authorised representative of the Subscriber and a Registration Operator from Worldline. The information that must be supplied for the request is specified in detail in subsection 4.1.1**Erreur ! Source du renvoi introuvable.**

This PC does not formulate any physical presence requirements but reserves the rights to have additional checks performed, such as phone calls for verification purposes.

An Organisation's private key is generated in a dedicated secure piece of equipment (Hardware Security Module) that has been certified in accordance with the FIPS 140-2 specification, level 2 or higher.

1.4.3 Test certificates

For technical purposes (i.e. testing whether the service is present and works), or for the demonstration and acceptance tests of the changes made to the production information system, the issuance of test certificates by the production **OTU CA** is allowed. Test certificates may in no way be used to hold the Holder, Subscriber or Worldline liable in the same way a production certificate does. However, for the Holder, Subscriber and CA, the obligations pertaining to the protection and use of the certificate are the same as those applicable to production certificates.

For these test certificates, it is imperative that the *CommonName* attribute of the « Subject » field be prefixed with the word “TEST”. These certificates must be revoked as soon as they are no longer needed.

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

1.5 Use of certificates

1.5.1 Areas of use

1.5.1.1 Key pairs and certificates

This CP concerns the key pairs and the associated electronic certificates that are managed by the certificate Holder mechanism identified in subsection 1.3.5, and which enable electronic certificate Subjects to sign or seal PDF documents as part of paperless contracting or transmission processes.

1.5.1.2 Key pairs, CA certificates and component certificates

The **OTU CA** has a single key pair that is used exclusively to sign Subject certificates, Organisation certificates, and CRLs. Its certificate is signed by the upper-level CA; see subsection 1.3.2.

The certification chain of the OTU PKI is the following:

- The certificate of the root CA is a self-signed AWL-RACINE electronic certificate.
- A certificate of a child CA is an electronic certificate delivered to a CA by the Root CA.
- A Holder certificate is an electronic certificate delivered by a child OTU CA and managed by the Holder mechanism.

1.5.2 Prohibited uses

Any use of a certificate issued by the OTU CA that contravenes the uses described in paragraph 1.5.1.1 and section 4.5 of this CP is prohibited.

The **OTU CA** may not be held liable if a certificate that it issues as per this CP is used for any other use than those specified in paragraph 1.5.1.1 and section 4.5 of this CP.

1.6 CP management

1.6.1 Entity that manages the CP

Worldline is responsible for drawing up this CP maintaining it, and revising it as soon as necessary. For this purpose, the security committee will make regularly make decisions as to the necessity of making changes to this CP.

1.6.2 Contact

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

Comité "MediaCert OTU"
Worldline
19, rue de la Vallée Maillard
B.P. 1311
41013 Blois Cedex
France

dlfr-mediacert-ac-otu@atos.net

1.6.3 Entity that determines whether a CPS complies with this CP

Worldline has the compliance of the CA verified by external auditors.

1.6.4 CPS compliance approval procedure

Worldline appoints the people who determine whether the CPS complies with this PC. These people are Worldline employees.

1.7 Definitions and Abbreviations

1.7.1 Main definitions

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

Authentication: electronic process that makes it possible to confirm the electronic identity of a natural or legal person, or the origin or integrity of electronic data.

Certificate: standardised X509 data element that makes it possible to associate a public key with its possessor. A certificate contains data such as

- its possessor's identity,
- its public key,
- the identity of the organisation that issued it (CA),
- its validity period,
- a serial number
- a thumbprint, and
- usage criteria.

All these elements are signed by the CA.

Certificate Holder mechanism: software component that obtains one or more certificates from the CA. These certificates are used for electronic signature purposes according to the applications and types of certificates.
The certificate Holder mechanism consists of servers that are operated at the same time as the CA. It guarantees the exclusive control of the key pairs by this entity only.

Certificate request: request that the Subscriber sends to the Registration Authority to obtain a certificate for the Subscriber's Customer. It includes information that must be supplied to the Registration Authority along with the certificate request.

Certification status information service: see paragraph 1.3.3.4

Certificate template: computer data resulting from the Registration of a Subscriber that requests a certificate from the Registration Authority. These data are then sent to the Certification Authority so they can be signed.

Certification Authority (CA): see subsection 1.3.3. The CA is the authority in charge of implementing this CP. It also refers to the technical entity that produces the certificates at the request of the Registration Authority, and more generally is in charge of managing them (manufacturing, delivery, revocation, publishing, logging and archiving) in accordance with the CP.

Certification Policy (CP): published document that describes all the rules defining the requirements which the CA abides by when setting up and providing services, and which specifies whether a certificate is applicable to a particular community or category of applications with common security requirements. If need be, a CP can also identify the obligations and requirements applicable to the various participants as well as all the components involved in managing the life cycles of certificates.
The certification policy is identified by an OID.

Certification Practice Statement (CPS): identifies the practices (organisation, operational procedures; and technical and human resources) that the CA implements when providing users with its electronic certification services in accordance with the certification policy/policies which it undertakes to abide by.

Child CA certificate: type of certificate delivered by the root OTU CA to sign the certificates and CRLs of child CAs.

Common Name (CN): element of the "Subject" field of the certificate which contains the identity of its possessor

Distinguished Name (DN): X500 distinguished name for which the certificate is issued. The DN consists of data, including the CN, which make it possible to know the Subject's identity precisely and unequivocally.

Electronic registration file: electronic data container designed to contain all the data sent by a Subscriber when the latter requests a certificate (certificate information, subject identification data, etc.). These data are archived in an archiving system with evidentiary value that the CA can access at any time.

Electronic seal: electronic data that are logically attached to or associated with other electronic data to guarantee their origin and integrity

Electronic signature: electronic data that are logically attached to or associated with other electronic data, and which the signatory uses to sign documents in accordance with the eIDAS European Regulation.
The French Civil Code gives the following definition: "*The signature identifies the person who uses it, indicates consent and guarantees the integrity of the document which it is attached to"*.
The electronic signature implemented in this CP does not comply with the definition of qualified signature.
The legal effect and admissibility of an electronic signature as legal proof cannot be refused for the sole reason that this signature is electronic or does not meet the requirements of the qualified electronic signature.

Electronic signature certificate: electronic proof that associates the validation data of an electronic signature with a natural person and confirms at least this person's name or pseudonym.

Hash: refers to the result of a calculation performed on digital content so any change made to this content, even the slightest one, also alters the hash. The hash is used to identify data and verify their integrity over time.

Holder certificate: type of certificate that a child CA delivers to Subjects or Organisations.

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

Lightweight certificate policy (LCP): certification policy that provides a service quality that is less costly than that achieved with the certification policies for qualified certificates as defined by [ETSI].

Organisation: entity that represents a company or is authorised to use a brand name for which a sealing certificate will be delivered at the request of a Subscriber

OTU certificate: one-time-use certificate that is produced dynamically during the online contracting process. This certificate is used by the platform during a single signing session (signing of the various documents of a contract for the Subject), after which the signing key is destroyed. It is delivered by a Certification Authority that signs the certificate containing identity of the Subject specified on it. This identity must have been verified by the Subscriber. This Subject can be a natural person who acts for their own needs or those of their Organisation, which must have duly authorised the Subject to do so.
The certificate provided by the this CA is not a qualified one.
The certificate is valid for a period that is specified on it.

PKI component: hardware platforms (computers, HSMs, chip readers) and software products that play specific roles within the PKI

Registration Authority (RA): see subsection 1.3.4. The RA is the authority in charge of receiving certificate requests from the Subscriber, verifying them, archiving them and sending them to the Certification Authority. This term also refers to the technical entity in charge of implementing the Registration service.

Registration service: see “Registration Authority”

Relying Party: in the context of this CP, the relying party is the entity that uses the certificate that it receives (here through an electronic signature). This signature is associated with a digital document (e.g. PDF document).

Revocation management service: see paragraph 1.3.3.3

Sealing certificate: electronic certificate used for sealing purposes

Signatory: natural person identified in one or more electronic documents and who creates an electronic signature for the aforementioned document(s).

Signing session: operation that takes place between the signing request and the return of the signed document(s) by the natural or legal person that is referred to in the request. During a signing session, several successive signing operations can be performed with the same certificate.

Subject: natural person identified in the certificate as its possessor. The certificate Holder mechanism generates and has exclusive use of the private key that is associated with the public key specified in the certificate.

Subscriber: entity that has signed a subscription contract with the **OTU CA** for the delivery of

- Organisation certificates at the request of duly authorised people within the Subscriber, or
- One-time-use certificates on behalf of Subjects as defined in this CP and whom the Subscriber will have identified beforehand.

The Subscriber is in direct contact with the RA and performs verifications on its behalf, notably about the identity and possible attributes of the Subjects that use certificates.

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

Trust chain: set of certificates required to validate the origin of a certificate delivered to an entity. In the context of this CP, the trust chain consists of the **OTU CA**'s certificate.

User: see Relying Party

1.7.2 Abbreviations

The acronyms used in this CP are

- **ARL:** Authority Revocation List
- **CA:** Certification Authority
- **CC:** Common criteria
- **CN:** *Common Name*
- **CO:** Certification Operator
- **CP:** Certification Policy
- **CPS:** Certification Practice Statement
- **CRL:** Certificate Revocation List
- **CSR:** Certificate Signing Request
- **DN:** Distinguished Name
- **ECSP:** Electronic Certification Service Provider
- **ETSI:** European Telecommunications Standards Institute
- **FQDN:** Fully Qualified Domain Name
- **HSM:** Hardware Security Module
- **ISO:** Information Security Officer
- **ISS:** Information System Security
- **KC:** Key Ceremony
- **OID:** Object Identifier
- **OTU CA: Certification Authority that delivers the certificates described in this CP**
- **PKI:** Public Key Infrastructure
- **PP:** Protection Profile
- **PS:** Publication Service
- **RA:** Registration Authority
- **RCA:** Root Certification Authority
- **RFC:** Request For Comment
- **RO**: Registration Operator
- **RSA:** Rivest Shamir Adelman
- **SHA:** Secure Hash Algorithm
- **SSL:** Secure Sockets Layer
- **TA:** Timestamping Authority
- **TLS:** Transport Layer Security
- **URL:** Uniform Resource Locator
- **UTC:** Universal Time Coordinated

1.8 Compliance statement

This CP complies with the LCP level of technical specification [ETSI102 042].

2 Responsibilities with regard to the information that must be published

2.1 Entities in charge of making the information available

To provide the information that must be published for certificate users, the CA implements a publication function and a certificate status information function.

This CP is available publicly.

The CRL is available publicly.

2.2 Information that must be published

The **OTU CA** publishes the Certificate Revocation List (CRL) using the HTTP protocol.

The **OTU CA** publishes this certification policy.

The URLs for accessing the CP and the CRL are available in extensions of the certificates delivered by the **OTU CA** (see "Profile" in section 7.1). These extensions are respectively

- “CPS URI”, and
- “CRL Distribution Point”.

The **OTU CA** publishes on its website (http://www.mediacert.com) the certification documents that are available and provided by an approved Organisation.

2.3 Publication time and frequency

The time and frequency at which the certificate status information is published, and the availability requirements applicable to this information, are specified in subsection 4.8.1 and section 4.10 of this document.

The CP that is publicly available is the most recent one in force.

2.4 Access restrictions applicable to the published information

The CRL and CP are read-only documents.

2.4.1 Access to the other documents

Write access to the systems used to publish information about the statuses of certificates (i.e. adding, deleting or modifying the published information) is strictly limited to the authorised internal functions of the **OTU** PKI through authentication on dedicated access control servers.

Write access to the other information is strictly limited to the authorised internal administration functions of the **OTU**. Access control is performed by dedicated servers.

The CPS specifies the access control resources that are implemented.

2.4.2 Monitoring of the Web page

The page containing the published information has a high availability rate. The required availability rate of this page is 99.8%.

The site is monitored by teams of the Atos group.

2.4.3 Document authenticity verification

The documents uploaded to the Mediacert site are authentic and certified as such by the presence of an electronic signature.

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 X509v3 certificate, the "Issuer" and "Subject" fields are identified using X.501 "Distinguished Names" (DN) in the form of printable strings ("PrintableString").

3.1.2 Necessity of using explicit names

In the case of a one-time-use certificate, the certificates issued according to this CP explicitly contain the Subject's name and forename.
In the case of Organisation certificates, the issued certificates contain

- the explicit name and forename of the individual who has been authorised by the Subscriber, and
- the Organisation's name.

3.1.3 Anonymisation or pseudonymisation of Holders

The notions of anonymisation or pseudonymisation are not used.

3.1.4 Rules for interpreting the various name forms

The interpretation of the information contained in the DN field is explained in the "Certificate Profiles" chapter of the **OTU CA**'s CP (see chapter 7).

3.1.5 Name uniqueness

The "Distinguished Name" (DN) field is unique for each Subject or Organisation. Any request that does not comply with this rule is refused. Therefore, throughout the life span of the CA, a DN that has been assigned to a Holder or Organisation cannot be assigned to another Subject or Organisation. Paragraph 7.1.2.2 specifies the rules that are applied to achieve such name uniqueness.

- For one-time-use certificates, name uniqueness is guaranteed throughout the life cycle of the CA. Therefore, if a Subject requests two distinct certificates through the Subscriber, two different DNs will be issued.

- For Organisation certificates, the uniqueness of the DN is guaranteed by the Registration Operator during the Registration. For the same Organisation, the DN will not change when certificates are renewed.

3.1.6 Identification, authentication and role of registered trademarks

See paragraph 3.2.2.2

3.2 Initial identity validation

3.2.1 Method for proving the possession of the private key

3.2.1.1 One-time-use certificate

For certificates designed to be used over short periods of time, the possession of the key is verified by means of a low-level cryptographic check of a first signature produced using the private key.

If this check fails, the PDF document is not signed, the private key is destroyed, and the Subscriber who has made the request receives an error message saying that the request has failed.

The certificate Subject is not subjected to this proof of possession.

3.2.1.2 Organisation certificate

The proof of possession of the private key supplied by the certificate Holder mechanism is guaranteed during the generation of the request. This is achieved through the signing of the message with the private key that corresponds to the public key contained in the PKCS#10 message sent to the RA.

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

The authorised individual specified on the certificate is not subject to this proof of possession.

3.2.2 Validation of Organisations' identities

3.2.2.1 Initial validation of the Subscriber

The initial validation of a Subscriber is associated with the prior establishment of a contractual relationship between the Subscriber and Worldline. This is the Contract through which the Subscriber subscribes to the OTU electronic signature service, the electronic certificate service, or the server certificate service.

A representative of the Subscriber must be declared to the CA. This representative of the Subscriber can be

- the Subscriber's legal representative (as specified on a Subscriber's company registration certificate less than three months old),
- the Subscriber's conventional representative (e.g. as specified in the company's statutes), or
- a representative whom the legal representative has allowed to represent the Subscriber as part of the execution of the Subscription contract.

This representative of the Subscriber will subsequently be the CA's contact for Organisation certificate requests.

Through its legal or statutory representative, the Subscriber can formally appoint one or more deputy Subscriber representatives who are also allowed to represent the Subscriber. To do so, The Subscriber must inform the CA and give these representatives the necessary power.

During the implementation of the subscription contract, the representative appointed by the Subscriber will have to supply

- a copy of a valid official identity document (French national ID, passport or residence card). The RA will keep a copy of this document.
- a company registration certificate less than three months old containing the representative's name and capacity, or the statutes of their Organisation, and all the valid documents required to prove the representative's authority;
- If the representative does not appear on the company registration certificate or the published statutes, the Subscriber's legal representative will have to duly authorise them to represent the Subscriber by means of a written proxy indicating the powers vested in them.

They will also have to supply an e-mail address that will be used to contact them, notably to send information to them during the creation of organisation certificates.
When the Subscriber's representative requests an Organisation certificate, this representative is authenticated by the Registration Operator.

When they request one-time-use certificates from the RA, the Subscriber's representative will have to authenticate themselves and sign these requests electronically.

When requesting signatures from the certificate Holder mechanism, the Subscriber will have to authenticate itself and sign these requests electronically.

It is imperative that the Subscriber use the authentication and signing methods required by the RA and the certificate Holder mechanism.

The certificates that the Subscriber uses to authenticate itself, and sign the certificate and signing requests must be issued by a certification authority approved by the **OTU CA**.

The CPS describes the Subscriber authentication method, which is based on

- the use and verification of the electronic certificates with the RA and the certificate Holder mechanism, and
- the verifications carried out.

The RA keeps all the documents sent during this subscription operation.

3.2.2.2 Validation of an Organisation

As explained in subsection 1.3.8, the Organisation is represented by an authorised individual. The Subscriber must supply the following information:

<u>About the Organisation</u>

- Any document that is valid at the time of the certificate request and which proves the existence of the Organisation e.g.

  - a Company registration certificate less than three months old;
  - the original or copy of any deed or extract of an official register less than three months old and which specifies the company's name, its legal form, the address of its headquarters, and the identities of the associates and directors specified in paragraphs 1 and 2 of article R. 123-54 of the French Commercial Code or equivalent legislation in foreign law).

- The Organisation's statutes.

<u>Subscriber's right to have the Organisation's name appear on the certificate</u>

- Any document that is valid at the time of the certificate request and which proves the Subscriber's right to have the Organisation's name appear on the certificate. If the certificate is intended for the Subscriber itself (same name as the Organisation), this document is not required.

<u>The Subscriber's right to have the Organisation's name appear on the certificate can be based on</u>

- a signed request less than three months old made by an authorised representative of the Subscriber. This request must specify:
  - the name of the Organisation that must appear on the electronic certificate, and
  - the name and forename of the individual who is authorised to represent the Organisation and is identified on the certificate.
  - The authorised individual must also sign this request to express their acceptance.

- any document that is valid at the time of the certificate request and which makes it possible to prove that the authorised individual belongs to the Organisation.

- a copy of a valid official identity document of the authorised individual (French national ID, passport or residence card). The RA will keep a copy of this document.

- the postal address, e-mail address and phone number that the CA can use to contact the authorised individual.

The RA keeps all the documents sent as part of this request.

This CP does not formulate any physical presence requirements. However, the RA may carry out additional checks by phone.

3.2.3 Validation of an individual's identity

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

The Subscriber requests the certificate from the RA on behalf of the Subject. The Subscriber's request is made electronically.

The Subscriber creates the request and signs it with an electronic signature.

At the very least, the Subscriber's request must contain the following identification data about the Subject:

- the Subject's name and forename, and
- the Subject's title.

The Subscriber may also specify the following elements for the registration file:
- the Subject's postal address,
- the Subject's phone number,
- the Subject's e-mail address, and
- the Subject's date and place of birth.

Although this information is not contained in the produced certificate, it will be kept in the electronic registration file associated with the issuance of the certificate.

Keeping these data is necessary since they are needed to create the registration file that will be associated with each certificate issuance operation. This registration file contains these data, which describe the processes and data for identifying the final customer.

The certificate template as described in paragraph 7.1.2.2 defines how the uniqueness of the name is guaranteed on the certificate.

The Subscriber must tell the AC in writing the reliable user identification method that it will use to verify the civil identity declared by the future Subject.

These identification methods must at least involve the verification of a valid official document containing the Subject's photograph, or any other valid official method that makes or has made it possible to verify the declared identity of a Subject prior to the delivery of a certificate.
Notably, the elements that must be collected, verified and kept are

- the person's name, forenames, date and place of birth;

- the nature of the delivered document;

- the date on which and the place where the document was delivered;

- the name and capacity of the authority or person that delivered it, and possibly authenticated it.

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

Use of electronic identity data

- In certain countries, the identification step can be carried out using an electronic ID or other electronic methods recognised as legally valid ways of providing reliable identification.
- In this context, the Subscriber makes sure that the Subject holds a valid electronic ID or has other electronic methods recognised as legally valid ways of providing reliable identification.
- These methods will back up the identification data that the Subscriber will obtain from the Subject beforehand.

The Subscriber has documented the identification process in a written document beforehand, during its subscription request.

The document that describes the identification process is completed by information that makes it possible to determine the method used to obtain the Subject's consent to sign documents electronically with a one-time-use certificate. The methods for expressing and obtaining the Subject's consent can be

  - an electronic capture of a handwritten signature,
  - the entry of a code received via SMS on a mobile phone, or
  - a recording of the Subject's voice.

The above list is not exhaustive.

The process can be implemented by a technical Operator working on behalf of the Subscriber.

Since the identification process is described by the Subscriber, the latter will have to
- implement it (or have it implemented by its technical service provider); and
- send, in an electronic registration file, the identification data captured during the implementation of the selected process.

The CPS describes the implementation of the electronic registration file that will be created on this occasion.

The CA reserves the right to assess the reliability of the identification process and not to deliver certificates if the reliability of this process is deemed insufficient.

The Subscriber sends to the RA digital copies of the identity verification data except in the following cases:

The Subject belongs to the Subscriber's organisation

If the Subject belongs to the Subscriber's Organisation, the Subscriber will not have to carry out any extra identity checks if the Subscriber provided the Subject with a reliable authentication method, notably to access their professional mailbox or to log in to the application that requires their signature.

In such a context, the Subscriber asks the Subject that belongs to its Organisation to ensure the security of their computer, professional mailbox, and credentials.

The CA and the RA will have to make sure that the Subject did belong to the Subscriber's organisation at the time of the signature by means of sampling inspections.

The Subscriber does not send the RA the copies of identity verification elements

If the Subscriber verifies the Subject's identity, and the copies of the elements used to establish this identity have not been sent to the RA, the CA and the RA will have to make sure, by means of sampling inspection, that the Subscriber did carry out this verification.

The Subscriber will have to store these elements securely and will hold them on behalf of the CA, which will carry out the necessary verifications with the CNIL (*French data protection authority*) so it can meet the obligations that Certification Authorities have towards their Auditors.

All the data are archived electronically and kept in accordance with section 5.4.

3.2.3.2 Registration by a Registration Operator

RA agents can use the RA to process Organisation certificate requests.

3.2.4 Unverified information

All the information of the "Subject" field of the certificate is verified during the certificate request

However, the e-mail address supplied during a certificate request is not verified.

3.2.5 Validation by the Authority of the Subscriber that makes a request

The Subscriber authenticates itself with the RA before any request. The method for doing so differs according to the type of certificate that is requested:

- For a one-time-use certificate, certificate-based authentication is used.
- For an authentication certificate, the authentication is carried out by the Registration Operator.

3.2.6 RA validation

The RA authenticates itself with the CA before any request.

3.2.7 Interoperability criteria

This CP formulates no requirements in this regard.

3.3 Identification and validation of a key renewal request

3.3.1 One-time-use certificate

Under this CP, there is no key renewal function for this type of certificate.

3.3.1.1 Identification and validation for common renewal

Not applicable

3.3.1.2 Identification and validation for renewal following revocation

Not applicable

3.3.2 Organisation certificate

A renewal request is processed like a creation request. Therefore, no new Holder certificate can be supplied unless the corresponding key pair is renewed as well (see section **Erreur ! Source du renvoi introuvable.**).

3.3.2.1 Identification and validation for common renewal

Identification and validation for the common renewal of a Holder certificate are carried out in accordance with section 3.2.

3.3.2.2 Identification and validation for the renewal of a certificate following revocation

Identification and validation for the renewal of a certificate following revocation are carried out in accordance with section 3.2.

Under this CP, renewal and revocation do not have to be carried out simultaneously; however, a reasonable maximum period must be observed.

The Subscriber must inform the CA of the fact that the certificate has been renewed following revocation.

The following revocation cases (see 4.9.1.2) make the renewal of an Organisation certificate impossible:

- end of the Organisation's or Subscriber's activity, and
- end of the contractual relationship between the Subscriber and the CA.

3.4 Identification and validation of a revocation request

3.4.1 One-time-use certificate

When a certificate with a life span of 15 minutes is used, revocation can only take place when this certificate is used during a signing session. This is why a Subject's certificate can only be revoked at the request of the certificate Holder mechanism as described in section 4.9 .The request is sent to the RA.

The request is sent from the RA to the CA, which carries out the revocation in real time.

This CP does not impose any requirements regarding the identification of the certificate Holder mechanism that requests the revocation of a certificate.

3.4.2 Organisation Certificate

An Organisation certificate can be revoked by the following roles:

- the Authorised individual specified on the certificate or a person whom they may have appointed, and
- the CA that issued the certificate. The operation is then carried out by a Registration Operator of the CA under the supervision of a CA manager.

The revocation request is made in accordance with section 4.9.

4 Operational requirements concerning the life cycle of certificates

4.1 Certificate request

4.1.1 Origin of a certificate request

4.1.1.1 One-time-use certificate

Only a Subscriber identified by the CA is allowed to request the creation of a one-time-use certificate.
For this purpose, the Subscriber must have obtained the Subject's express consent beforehand. The Subscriber must have met this obligation before making any request to the CA.

4.1.1.2 Organisation Certificate

Only a Subscriber is allowed to request the creation of an Organisation certificate.
If the individual is not the legal or statutory representative, the Organisation will have to send the RA a written authorisation so this individual can appear on the Organisation certificate. Moreover, this authorised person must have given their signed consent beforehand and must be duly identified by the RA.

4.1.1.3 Registration of the Subscriber

During the process of subscription to the service, the **OTU CA** identifies the Subscriber and informs it beforehand of its obligation to identify its Subjects if the OTU electronic signature is implemented.

The Subscriber signs a subscription contract that will be saved and kept by the **OTU CA**.

The **OTU CA** authenticates Subscribers' requests and checks whether these Subscribers are allowed to request certificates.

4.1.2 Processes and responsibilities when drawing up a certificate request

4.1.2.1 One-time-use certificate

Paragraph 3.2.2.1 specifies the information that the request must include at the very least.

The Subscriber draws up the request on the basis of information that it will obtain from the Subject in a reliable way.

Through a signed agreement with the AC, the Subscriber undertakes to

- implement one or more processes for verified Subject identification,
- ask the CA in writing for its opinion about the identification processes that are implemented,
- tell the Subject about the various steps that they will have to follow to obtain certificates that bear their name so they can sign electronically the document that the Subscriber will submit to them,
- implement one or more processes to obtain the Subject's explicit agreement so the Subscriber can request a certificate from the RA on their behalf, and
- provide all the information required for the certificate to be issued.

The request is sent directly to the RA, which sends it to the CA.

The CA may not he held liable if the Subscriber does not honour its commitments to the CA.

The CA reserves the right to refuse to issue the certificate if the Subscriber fails to meet its obligations.

4.1.2.1 Organisation Certificate

Paragraph 3.2.2.2 specifies the information that the request must include at the very least.

The request file is drawn up by the authorised representative of the Organisation. The document is sent to the RA directly.

Besides, the RA makes sure that it has information that it can use to contact the future certificate Subject if need be.

The CA may not be held liable if the Subscriber does not honour the commitments specified in the Contract signed with the CA.

The CA reserves the right to refuse to issue the certificate if the Subscriber fails to meet its obligations.

4.2 Certificate request processing

4.2.1 Execution of request identification and validation processes

4.2.1.1 One-time-use certificate

The Subscriber's and the Subject's identities are verified in accordance with the requirements set out in subsection 3.2.2.

The RA

- validates the Subject identification data (i.e. ensures the correct data are present),
- verifies the Subscriber's identity and makes sure the RA knows the Subscriber, and
- makes sure the Subscriber has signed its request electronically with its name.

After performing these operations, the RA sends the certificate generation request. The RA then keeps a trace of the Subscriber's request in an electronic archive.

The CA will produce a certificate containing the Subject's identification data.

4.2.1.1 Organisation certificate

The identities of the Organisation and the individual authorised to represent it are verified in accordance with the requirements set out in subsection 3.2.2.

The RA

- validates the identification data of the Organisation and the authorised individual within the Organisation (completeness, accuracy), and
- makes sure that the request file is complete.

After performing these operations, the RA sends the certificate generation request. The RA then keeps a trace of the request in an electronic archive.

4.2.2 Acceptance or rejection of the request

If the request is rejected, the RA informs the Subscriber and justifies the rejection.

4.2.3 Certificate generation time

Certificate requests are processed "in real time".

For Organisation certificates, a specific document is created; it summarises the generation of the certificate and lists the technical personnel involved. This document is kept as execution log.

4.3 Certificate delivery

4.3.1 CA's actions with regard to certificate delivery

After authenticating the origin of the request and verifying the integrity of the request coming from the RA, the CA triggers the certificate generation processes. Chapters 5 & 6 set out the conditions under which keys and certificates are generated, and the security measures that must be complied with. The CA then sends the generated certificate to the certificate Holder.

4.3.2 CA's notification of the delivery of the certificate to the certificate Holder mechanism

After processing the certificate request, the CA sends the certificate to the certificate Holder mechanism through the RA. This transmission operation, which is logged in the RA's logs, has the same value as a notification.

In the case of an Organisation certificate, the latter is also sent to the Subscriber for explicit validation before use.

4.4 Certificate acceptance

4.4.1 Certificate acceptance process

4.4.1.1 One-time-use certificate

The Subject identification data used to generate the electronic certificate are validated explicitly by the Subject before the electronic certificate is used for the first time.

In addition, checks carried out by the certificate Holder mechanism make it possible to detect non-conformities and revoke the certificate that has been produced if it does not match the Subscriber's request.

4.4.1.2 Organisation certificate

The Organisation certificate produced by the CA is sent to the Subscriber for validation before use.

This CP requites that the certificate be accepted explicitly, either by the legal or statutory representative of the Subscriber that makes the request, or by the authorised individual identified on the certificate.

Acceptance via e-mail is considered as sufficient. The e-mail address is specified during the subscription request.

The sender's e-mail address is used to authenticate the origin of the acceptance of the certificate.

The certificate Holder mechanism cannot use any Organisation certificate in any way whatsoever without this acceptance phase.

4.4.2 Certificate publication

There is no service for publishing the certificates issued by the **OTU CA**. Only the **OTU CA**'s certificate is published.

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

Not applicable

4.5 Key pair and certificate uses

4.5.1 Use of the private key and certificate by the certificate Holder mechanism

The use of the private key and the associated certificate by the certificate Holder mechanism is strictly limited to the signing service described in section 1.5. Otherwise, the Holder may be held liable.

The authorised use of the key pair and the associated certificate is specified on the certificate by means of the key usage extensions.

4.5.2 Use of the private key and certificate by relying parties

Users and Subscribers must take into account the use specified on the certificates produced by the **OTU CA** (see previous subsection) and refuse any other use. Otherwise, they may be held liable.

4.6 Certificate renewal

Certificate renewal (i.e. generation of a new certificate without a key change) is prohibited by this CP.

4.6.1 Possible reasons for certificate renewal

Not applicable

4.6.2 Origin of a renewal request

Not applicable

4.6.3 Renewal request processing

Not applicable

4.6.4 Notification of creation of a renewed certificate

Not applicable

4.6.5 Acceptance of the new certificate

Not applicable

4.6.6 Publication of the new certificate

Not applicable

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

Not applicable

4.7 Delivery of a new certificate a change of key pair

In the context of the delivery of one-time-use certificates, the delivery of a new certificate is not applicable.

For Organisation certificates, the delivery of a new certificate is handled like a creation request. A new key pair is generated systematically.

The use of an existing key pair associated with a former CSR is prohibited.

4.7.1 Possible reasons for a change of key pair

In the context of Organisation certificates, Organisations' key pairs and the associated certificates are renewed every 3 years. A key pair and a certificate can be renewed in advance following the revocation of the Holder's certificate (see section 4.9, and notably subsection 4.9.1 for the possible reasons for revocation).

It should be noted that the following reasons for revocation (see paragraph 4.9.1.2) result in the prohibition of delivery of new certificates:

- ceasing of the Organisation's activity, and
- end of the contractual relationship between the Organisation and the CA.

4.7.2 Origin of a request for a new certificate

See paragraph 4.1.1.2

4.7.3 Processing of a request for a new certificate

See paragraph 4.2.1.1

4.7.4 Notification of creation of the new certificate

See subsection 4.3.2

4.7.5 Acceptance of the new certificate

See paragraph 4.4.1.2

4.7.6 Publication of the new certificate

See subsection 4.4.2

4.7.7 Notification sent by the CA to inform other entities of the delivery of the new certificate

See subsection 4.4.3

4.8 Certificate modification

Certificate modification is prohibited by this CP.

4.8.1 Possible reasons for a change of key pair

Not applicable

4.8.2 Origin of a request for a new certificate

Not applicable

4.8.3 Processing of a request for a new certificate

Not applicable

4.8.4 Notification of creation of the new certificate

Not applicable

4.8.5 Acceptance of the new certificate

Not applicable

4.8.6 Publication of the new certificate

Not applicable

4.8.7 Notification sent by the CA to inform other entities of the delivery of the new certificate

Not applicable

4.9 Revocation and suspension of certificates

4.9.1 Possible reasons for certificate revocation

The **OTU CA**'s Certification Policy prohibits certificate suspension since a revoked certificate cannot be made usable again.

4.9.1.1 One-time-use certificates

The following circumstances can result in the revocation of a Subject's certificate:

- The Subject's information that appeared on the certificate when it was issued does not match the Subject's identity or contravenes the use specified on the certificate.
- An intentional or unintentional error has been detected in the Subject's registration request.
- An incident occurred when the certificate Holder mechanism used the certificate for a signing operation in the context of the normal use provided for in section 1.4.
- The private or public keys do not match.

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

However, given

- the use of the one-time-use certificates produced in the context of this CP, and
- the short life span of such certificates,

it is important to note that revocation here is an instrument which, first and foremost, makes it possible to provide a CRL for technical components that must have one.

For one-time-use certificates, the reason for the revocation is not published.

4.9.1.2 Organisation Certificates

The following events can result in the revocation of the certificate:

- The Organisation's information that appeared on the certificate when it was issued does not match the Organisation's identity or the use specified on the certificate.
- An intentional or unintentional error has been detected in the Organisation's registration request.
- The Holder's private key is compromised or suspected of being compromised.
- The Holder's private key has been lost or stolen.
- The verification of the use of the Holder's private key is suspected of having failed.
- The information appearing on the certificate is no longer accurate although the certificate's expiry date has not been reached yet.
- The authorised representative (Subject / Organisation) requests the revocation of the certificate (notably if the private key has been destroyed or altered).
- The Organisation's or Subscriber's activity comes to an end.

- The contractual relationship between the Subscriber and the CA ends.
- Changes occur in the technical or legal regulations, or in the recommendations applicable to the CA or Organisation, thus requiring that the certificate no longer be used.

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

In addition, Worldline can revoke a certificate as of right under the following circumstances:

- A Subject or the Subscriber fails to meet any of the obligations resulting from the Subscription Contract or from any other document contained in the subscription file, notably if the certificate is used under conditions other than those provided for by this Certification Policy.
- failure to comply with this Certification Policy.

For Organisation certificates, the reason for the revocation is published, which makes it possible to identify the type of certificate in the CRL.

4.9.1.3 Certificate of a PKI component

The following events can result in the revocation of a certificate of a PKI component (including a CA certificate used to generate certificates or CRLs):

- The private key is compromised or suspected of being compromised.
- The private key is lost or stolen.
- The content has been altered following an upgrade (nonconformity correction, change made to the certificate template, etc.).
- cessation of activity, or
- regulatory changes in the algorithms used.

The decision to revoke a component of the **OTU** PKI is made by Worldline.

4.9.2 Origin of a revocation request

4.9.2.1 One-time-use certificates

Only the certificate Holder mechanism entity as described in subsection 1.3.5 is authorised to request the revocation of this type of certificate under the conditions set out in paragraph 4.9.1.1.

4.9.2.2 Organisation certificates

The people or entities that can request the revocation of a Holder certificate are

- an authorised representative of the Subscriber who has the identification / authentication data that enable them to access this function.
- the CA, according to the circumstances specified in paragraph 4.9.1.2, in which case a Registration Operator will perform the operation under the supervision of a representative of the CA.

4.9.2.3 Certificates of a PKI component

The revocation of a CA certificate or other component certificates can only be decided by Worldline or legal authorities following a court ruling. The revocation is carried out immediately.

4.9.3 Revocation request processing

4.9.3.1 Revocation of a one-time certificate

This CP does not impose any requirements concerning the identification of the revocation request. Indeed, only the certificate Holder as described in subsection 1.3.5, is authorised to request the revocation of such certificates on the basis of the possible reason for revocation that it has detected.

The operation is logged in the event logs.

4.9.3.2 Revocation of an Organisation certificate

A representative of the Organisation calls a number that is available 24 hours a day, 7 days a week.

A Pilot will ask for

- identification information (names of the Organisation and the authorised representative), and
- authentication information (secret code given during the generation of the certificate).

Once the identification and authentication data are validated, the revocation is authorised.

The operation is logged in the event logs.

The revocation of an Organisation certificate is carried out in several steps, some of which are done by phone with the customer (the latter being the person on the phone who requested that this procedure be initiated.) For each of these steps, the customer is the person who must specify the information to enter or verify.

Revocation requests are monitored and logged so compliance with the revocation period can be established.

4.9.3.3 Revocation of a certificate of a PKI component

In the **OTU CA**'s CPS, the CA specifies the procedures that must be implemented when a certificate of a PKI component must be revoked.

Refer to subsection 5.7.3 if one of the certificates of the certification chain is revoked.

4.9.4 Time given to the Subject to request the revocation

As soon as the authorised representative (Holder / Organisation) is aware of one of the possible reasons for revocation, they request the revocation immediately.

4.9.5 Time needed by the CA to process a revocation request

The maximum period of time between the revocation request and the moment relying parties (certificate users) are given the information is 72 hours.

4.9.5.1 Revocation of a Holder certificate

The revocation management function is available 24 hours a day, 7 days a week.

Any request for the revocation of a Holder certificate is processed immediately after the **OTU CA** has received it.

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

4.9.5.2 Revocation of a certificate of a PKI component

The revocation of a signature certificate of the CA is organised by Worldline.

This operation requires that the root CA be reactivated and that several roles be present. It can be performed within 48 working hours after the request.

4.9.6 Revocation request tracking

Since a revocation request is defined by the number of its ISMP modification and its revocation date, it can easily be tracked and traced. This makes it possible to check whether the revocation period has been complied with or not.

4.9.7 Requirements with regard to the verification of the revocation by certificate users

This CP does not impose any requirements with regard to the obligation to check whether a certificate has been revoked.

4.9.8 CRL publication frequency

CRLs are published every 24 hours.

4.9.9 CRL publication deadline

The CRL is published 5 minutes after its generation at the latest.

4.9.10 CRL archiving

The CRLs created by the **OTU CA** are archived.

The default retention time for CRL archives is 10 years.

4.9.11 Other ways of obtaining information about revoked certificates

Not applicable

4.9.12 Requirements with regard to the online verification of revoked certificates by certificate users

Not applicable

4.9.13 Other ways of obtaining information about revoked certificates

Not applicable

4.9.14 Specific requirements if the private key is compromised

The entities that are allowed to request the revocation of a certificate must do so as early as possible after being informed that the private key has been compromised.

For CA certificates, the revocation following the compromise of the private key is clearly specified in a statement on the CA's website.

4.9.15 Possible reasons for certificate suspension

This CP prohibits certificate suspension.

4.9.16 Origin of a suspension request

Not applicable

4.9.17 Suspension request processing

Not applicable

4.9.18 Minimum and maximum durations of the certificate suspension period

Not applicable

4.10 Certificate status information function

4.10.1 Operational characteristics

The certificate status information function enables certificate users to view public CRLs. The CRLS are in V2 format and published via HTTP at the address specified in the "CRL Distribution Point" extension of user certificates (see section 7.1).

The CRL contains the list of the certificates issued by the **OTU CA** which, at the same time, have been revoked and have not expired yet (the expiry date and time of the certificate have not been reached.).

A certificate that has been revoked or has expired is no longer contained in the CRL.

4.10.2 Availability of the function

The certificate status information function is available 24 hours a day, 7 days a week.

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

4.10.3 Optional mechanisms

This CP formulates no specific requirements in this regard.

4.11 End of the relationship between the Subscriber and the CA

The end of the relationship between the Subscriber and the CA is materialised by the cancellation or non-renewal of the subscription contract or the service contracts that are expressly associated with it.

The RA no longer recognises the requests sent and signed by the Subscriber.

The CA asks the Subscriber to immediately revoke its Organisation certificate if it uses one or more. This revocation can be verified through the certificate status information service provided by the OTU CA.

4.12 Key escrow and recovery

This CP prohibits the escrow of CA private keys and Holder certificates.

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

Not applicable

4.12.2 Policy and practices with regard to the recovery of session keys through encapsulation

Not applicable

5 Non-technical security measures

5.1 Physical security measures

The CPS specifies how the checks concerning the following elements are executed:

- geographical location,
- site construction,
- physical access,
- energy and air conditioning,
- exposure to fluids,
- fire security,
- media retention,
- media destruction, and
- offsite backup.

This aims to ensure that

- the means and information used for the operational implementation of the OTU PKI are installed on premises, the access to which is controlled and reserved for the authorised staff.
- the access control system guarantees the traceability of the access to the premises where the OTU PKI's resources and information are stored.
- the implementation of these checks makes it possible to comply with the separation of trusted roles provided for by this CP.

5.2 Procedural security measures

5.2.1 Trusted roles

The functions operated in all of the **OTU CA**'s components are distributed to various types of roles to ensure that knowledge is separated for sensitive tasks or roles. The various types of roles of the CA Organisation are notably:

- CA manager,
- Deputy CA Manager,
- Registration Operator,
- Security Manager,
- Application Manager,
- System Engineers,
- HSM Administrators,
- Secret Holders,
- Manager of the centre (that hosts the CA), and
- Witnesses (auditors).

These various roles are described in the document entitled "Table of roles and secrets" [ROLES_SECRETS] and in the Key Ceremony document for the people who have operational roles at that time.

Several roles can be held concurrently if this proves compatible with knowledge separation.

Measures are taken to prevent the equipment, information, media and software related to the **OTU CA**'s services from being taken out of the site without authorisation.

5.2.2 Number of people required per task

According to the type of operation, the number and roles of the people that must be present (as participants or witnesses) may differ.

5.2.3 Identification and authentication for each role

Each entity that operates a component of the PKI **OTU** verifies, for each of its components, the identity and authorisations of any staff member and external person who works on sensitive tasks. These verifications comply with the security policy of the component. A written notification is produced every time a role is assigned to a member of the PKI staff. This role is clearly specified and described in the staff member's job description.

5.2.4 Roles that require remit separation

Several roles can be assigned to the same person provided such concurrence does not compromise the security of the implemented functions.

The remit associated with each role complies with the security policy.

Holding the following trusted roles concurrently is prohibited:

- Security Manager and System Engineer,
- Security Manager and Registration Operator,
- System Engineer and Registration Operator, and
- Auditor and any other role.
- Secret Holders should they have secrets that contravene subsection 5.2.2, which would result in a situation that would reduce the number of people needed for an operation.

The people in charge of revoking and creating certificates must be independent of the Organisations when it comes to the decisions that they can make during these operations. They must also be free from any financial, commercial or other pressure that might affect their tasks and operations within the OTU CA.

5.2.5 Responsibilities of trusted roles

The responsibilities of trusted roles are defined and assigned. They can be found in the role assignment documents (CA Manager, Deputy CA Manager, and Registration Operator).

5.2.6 Inventory of secrets

The inventory of the **OTU CA**'s secrets is kept and carried out by a category of trusted person (Secret Holder).

5.3 Security measures with regard to the staff

5.3.1 Required qualifications, skills and authorisations

Any person involved in trusted roles of the **OTU** is informed of

- their relative responsibilities, and
- the system security and staff inspection procedures that they must abide by.

5.3.2 Criminal record verification procedure

Procedures for verifying criminal records are implemented for the people who are likely to hold sensitive roles. In particular, these people must not have been convicted or find themselves in a situation where a conflict of interest exists, which would contravene their remit. Failing that, the applicant's application will be subjected to the discretionary validation of the HR department and the OTU CA manager. The applicant can give their employer a copy of bulletin number 3 of their criminal record as part of the hiring procedure and when handing in their initial liability agreement.
Criminal records are verified every three years.

5.3.3 Basic training requirements

The staff are trained in the software, hardware and working procedures of the CA.
The staff know the consequences of the operations that they are in charge of.

5.3.4 Continuous training requirements and frequency

The staff concerned receive the necessary training before any change is made to systems, procedures, the Organisation, etc. according to the nature of these changes.

5.3.5 Frequency and sequence of assignment rotation

This CP formulates no requirements in this regard.

5.3.6 Disciplinary sanctions in case of fault

The by-laws of each entity indicate that appropriate administrative disciplinary sanctions are applicable in the event of a fault (failure to comply with this CP, etc.). The liability agreement reminds employees of this fact.

5.3.7 Requirements with regard to external providers' staff

External providers' staff working on the premises or components of the PKI must meet the requirements set out in sections 5.3.1, 5.3.2, 5.3.3 and 5.3.4.

5.3.8 Documents given to the staff

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

5.4 Procedures for constituting audit data

The events that occur in the life of the **OTU** CA are logged to files through automated software generation that is completed by manual data entry if need be. These files aim to ensure the traceability of operations (authors, timestamps, etc.).

The logging process is carried out in real time for automatic systems. For manual interventions, logging is performed, at the earliest, as soon as the operation is initialised.

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

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

5.4.1 Types of events logged

The PKI **OTU** logs the following events:

- start-ups and stops of IT systems;
- start-ups and stops of applications;
- start-ups, stops and modifications of the settings of the logging function;
- generation of keys for the various components;
- changes, corrections or upgrades of the various components;
- receipt of a certification or revocation request;
- validation or rejection of a certification or revocation request;
- generation of Holder certificates;
- transmission of certificates to the certificate Holder mechanism;
- certificate revocation;
- generation and then publication of CRLs.

Some security-specific events are:

- physical access to the premises that host the **OTU**;

- changes to the technical platform (maintenance, software upgrade);
- changes in the staff working on the **OTU**;
- purge or destruction operations;
- Pilots' monitoring and management actions;
- creation/modification/deletion of user accounts and the corresponding authentication data;
- logins/logouts of the users who have trusted roles, and the associated failed attempts;
- events related to signature keys and CA certificates (generation during a key ceremony, backup / recovery, revocation, renewal, destruction, etc.).

Logged events contain all the information that is needed to identify and analyse them:

- type of event or operation;
- date and time of the event;
- the people involved (software component or Operator's intervention);
- context (scheduled operation with a requisitioner, operational intervention subjected to a procedure following a malfunction, etc.);
- result (success or failure);
- possible relation to other events.

The person, Organisation or system that executed an action is accountable for it. The name or identifier of this person / Organisation / system is specified explicitly in a field of the event log.

5.4.2 Event log processing frequency

The event log processing frequency is specified in the CPS.

5.4.3 Event log retention period

The retention time for event logs is specified in the CPS.

5.4.4 Event log protection

Event log protection is described in the CPS.

5.4.5 Event log backup procedure

The event log backup procedure is described in the CPS.

5.4.6 Procedures for returning and verifying the return of event logs

The procedures for returning and verifying the return of event logs are described in the CPS.

5.4.7 Event log collection system

The event log collection system is described in the CPS.

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

Event logging notification is specified in the CPS.

5.4.9 Evaluation of vulnerabilities

Event log analysis is described in the CPS.

5.5 Data archiving

5.5.1 Type of data to archive

The archiving is carried out by the **OTU CA** to ensure the traceability and non-repudiation of operations. Notably, the data that must be archived are

- for the **OTU CA**'s CA and RA:
    - certificate generation requests,
    - revocation requests, and
    - certificates and CRLs.
- for the **OTU**'s technical platform:
    - the technical documents that describe IT configurations and equipment,
    - software operation settings,
    - operation procedure documents,
    - the daily operation register; and
    - event logs.
- for documents:
    - key ceremony manuals, and
    - versions and revisions of the CP and CPS.

5.5.2 Archive retention period

For the CA and the RA, the default retention time for registration file archives is 8 years from the moment the RA has validated these registration files.

However, this retention time can be modified:

- This duration can be lowered to 3 years at the Subscriber's request.
- If the contract with the Customer ends, the registration files can be returned to the Subscriber (still with a minimum duration of 3 years).
- The Subscriber can expressly request that this period be extended beyond eight years for the customer. This can only be justified by regulatory or legal constraints. Moreover, the people specified in the registration files must be informed accordingly.

For the technical platform, logs are kept for 8 years.

For documents, archives are kept for 3 years after the expiry of the OTU PKI.

5.5.3 Archive protection

The integrity of archives is protected during the retention period. The CPS specifies the measures taken to ensure their availability and make them viewable if need be.

Access to an archive is requested by the application manager or security manager.

5.5.4 Archive backup procedure

Backups benefit from the same level of protection as archives. The backup procedures and protection level are described in the CPS.

5.5.5 Data timestamping requirements

Timestamping requirements are specified in section 6.8.

5.5.6 Archive collection system

Archives are produced once a month. The CPS specifies the methods used to collect archives, and the associated protection levels.

5.5.7 Archive retrieval

Archives can be retrieved in less than two working days from the registration of the request.

5.6 Change of the CA's key

The **OTU CA**'s certificate will expire on 31/12/2020. The **OTU CA** cannot issue certificates whose validity dates (start or end dates) exceed its own expiry date.

As soon as the **OTU CA**'s new key pair is generated, only the new private key is used to sign certificates. The previous certificate can no longer used (even for CRLs).

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

5.7 Recovery following compromise and disaster

5.7.1 Procedures for reporting and handling incidents and compromises

The CA takes appropriate and organisational measures to manage the risks pertaining to the security of the trust services that are provided.
These measures guarantee that the security level is proportional to the degree of risk. Notably, measures are taken to prevent and mitigate the consequences of security-related incidents, and to inform the parties concerned of the detrimental effects of such incidents.

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

If the CA's equipment is damaged or out of order but the signing keys have not been destroyed, operation is restored as quickly as possible. Priority is given to the ability to provide services for revoking certificates and publishing their validity statuses (CRLs).

An incident simulation test including a stop of a component of the OTU PKI is done at least once every 3 years.

5.7.3 Recovery procedures should a component's private key be compromised

The compromise of an infrastructure key is dealt with in the component management document (see subsection 5.7.2) as a disaster.

If the **OTU CA**'s private key is compromised, suspected of being compromised, or destroyed

- After investigating the event, Worldline decides to revoke or not the **OTU CA**'s certificate.
- If the **OTU CA**'s certificate is revoked, all the generated Holder certificates are revoked.
- A new key pair is generated and a new **OTU CA** certificate is issued.
- Worldline decides on the communication plan intended for Subscribers and users of the CA's certificates.
- Within two working days, Worldline informs Adobe of the revocation of its **OTU CA** certificate.

5.7.4 Disaster recovery

The CPS describes the procedures that are implemented when a disaster occurs.

5.8 End of the PKI's life

5.8.1 Transfer or cessation of activity affecting a PKI component other than the CA

This CP prohibits the transfer of the CA to a third party.

5.8.2 Cessation of activity affecting the CA

If the CA decides to stop its activity, it must inform its partners at least six (6) months before this cessation of activity.

In such a situation, the **OTU CA**

- revokes the certificates that it has signed,
- revokes its certificate,
- informs entity representatives about the certificates that are or must be revoked,
- destroys its Authority key pair during an audited Key Ceremony-type procedure, and
- keeps images of its data and archives.

On the appointed date, the CA revokes all the certificates that it has produced and publishes a CRL.
Likewise, at root CA level, the **OTU CA** is revoked and an ARL is published.

The CRL published only once covers the revocation of certificates over their entire existence. Therefore, the duration of the CRL is set to 3 years.

This CRL remains online at the usual address for 3 years.

The **OTU CA** is not allowed to transmit its private keys.

6 Technical security measures

6.1 Key pair generation and installation

6.1.1 Key pair generation

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

6.1.1.1 CA keys

The CA's private key is used and is kept on the OTU PKI's premises (see chapter 5). The CA's key pairs are generated in an HSM that has been certified in accordance with the Common Criteria (CC) EAL 4+ certification.

Key ceremonies take place on the **OTU** PKI's premises, under the supervision of two (2) people (master of ceremony and auditor) and in accordance with scripts defined beforehand. The CA's private key is used and stays on the **OTU**'s secure premises.

The roles of the employees involved in key ceremonies are described in the CPS and the key ceremony document. The witnesses, one of whom is external to the CA and is impartial, testify to the proper execution of the ceremony on the basis of the key ceremony description document delivered beforehand.

6.1.1.2 Authentication keys of a PKI component

The keys that enable the components of the PKI to authenticate themselves are generated during the key ceremony (at the same time as CA keys or not). A document is created which describes the execution of the key ceremony and the required participants.

6.1.1.3 Subscribers' keys

The **OTU CA** does not produce the certificates associated with a Subscriber's private key. The CPS describes how the RA recognises the Subscriber.

The Subscriber is informed of the rules that it must abide by to authenticate itself with the RA.

It is Subscriber's responsibility to obtain the certificates that will enable it to authenticate itself with the CA.

It is not the **OTU CA**'s responsibility to deliver these certificates.

6.1.1.4 Keys of the Holder certificates generated by the CA

The **OTU CA** does not generate the keys of Holder certificates.

6.1.1.5 Keys of the Holder certificates generated for the Holder

The key pairs are generated by the certificate Holder mechanism, which has exclusive use of them.

The CA implements verification and protection methods in the certificate Holder mechanism to protect the use of the private keys.

The certificate Holder mechanism generates its key pair in an HSM that has been certified in accordance with the FIPS 140-2 specification, level 2 or higher; and in accordance with the requirements set out in section 7.1, notably with regard to key length.

6.1.2 Transmission of the private key to its owner

Not applicable

6.1.3 Transmission of the public key to the CA

The certificate Holder mechanism sends the **OTU CA** the public key to in a template in PKCS#10 (CSR) format so the certificate is generated.

6.1.4 Transmission of the CA's public key to the various participants

The certificate of the **OTU CA** is published at the following URL:

www.mediacert.com

6.1.5 Key size

The **OTU CA** uses the RSA algorithm with the SHA-2 hash function.

The size of the **OTU CA**'s key pairs is 2,048 bits.
The size of Subjects' and Organisations' keys is 2,048 bits.

6.1.6 Verification of the generation of key pair settings and their quality

The CA's key pairs are generated in an HSM that has the Common Criteria (CC) EAL 4+ level. The settings of the equipment that generates the key pairs (HSM) are described in the key ceremony document.

6.1.7 Target uses of the key

The use of the CA's private key and the associated certificate is strictly limited to the signing of certificates and CRLs (see paragraph 1.5.1.2).
The use of the private key of the Holder certificate is strictly limited to the signing service (see paragraph 1.5.1.1 and section 4.5).

The use of the "keyUsage" field in the Holder certificate is "Non-repudiation".

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

6.2.1 Security standards and measures for cryptographic modules

6.2.1.1 CA's cryptographic modules

The CA's key pairs are generated in an HSM that has the Common Criteria (CC) EAL 4+ level, which meets the requirements set out in section 10.4.

6.2.2 Private key control

The CA's private key is controlled by trusted staff (secret holders of the **OTU**, and HSM administrators) in a protected environment. The CA's signing private key is activated through a system that enables several roles to share secrets.

6.2.3 Private key escrow

The private keys of the **OTU CA**'s certificates and Holder certificates are not held in escrow.

6.2.4 Private key emergency backup

The private keys of Holder certificates (Subject and Organisation certificates) are not backed up.

The **OTU** CA's key pairs are backed up under the supervision of several people. The private keys are backed up with hardware cryptographic resources (HSMs).
The emergency backup procedures are described in the key ceremony document.

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

6.2.5 Private key archiving

The private keys of **OTU CA**s' and Holder certificates are not archived.

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

CA keys are generated and stored in hardware cryptographic resources (HSMs).

When the CA must transfer a private key to another HSM of the OTU PKI, the transfer is carried out in accordance with the specifications of the supplier of the **OTU CA'**s cryptographic hardware (HSM).

During a transfer, the private key is encrypted using the 3DES algorithms. A CA's private key that has been encrypted cannot be decrypted without the use of hardware cryptographic components and the intervention of the people identified as trusted role holders.

6.2.7 Storage of a private key into a cryptographic module

OTU CAs' private keys are stored into hardware cryptographic resources (HSMs) that meet the requirements set out in section 10.4. Therefore, the security level is the same as when these keys are generated.

6.2.8 Private key activation methods

6.2.8.1 CA's private keys

The **OTU CA**'s private keys can only be activated with two (2) people who have trusted roles and activation data. This activation can only be carried out as part of documented, logged key ceremonies.

6.2.8.2 Private keys of Holder certificates

The private keys of Holder certificates are generated and stored into hardware cryptographic equipment (HSM) that has been certified in accordance with the FIPS 140.2 specification, level 2 or higher.

The keys of OTU certificates are generated dynamically, at the RA's order, in a single HSM used for a single signing session. They are then destroyed in this HSM. This sequence of operations is logged in the PKI's logs.

The keys of Organisation certificates are generated by OTU CA operators during a key generation operation that is documented and logged. The key is copied onto the other dedicated HSMs used for the same purpose. This is done using the cloning processes recommended by the HSM supplier.

6.2.9 Private key deactivation method

6.2.9.1 CA's private keys

The CA's private keys stored in the HSM are automatically deactivated as soon as the latter is stopped or disconnected. HSMs are stored in a secure area kept under control.

6.2.9.2 Private keys of Holder certificates

The private key of the OTU certificate is destroyed after use.

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

6.2.10 Private key destruction method

6.2.10.1 CAs' private keys

OTU CAs' private keys and their backup copies are destroyed through deletion from the HSM. When the life of a CA's private key ends, whether normally or early (revocation), this key is systematically destroyed as well as any copy and element that makes it possible to rebuild it.

6.2.10.2 Private keys of Holder certificates

The private keys of OTU certificates are destroyed after a single use in accordance with section 1.5. The destruction is logged by the certificate Holder mechanism.

6.2.11 Evaluation of the cryptographic module

The cryptographic and backup resources of the **OTU's** CAs are evaluated in accordance with the requirements set out in section 10.4.

6.3 Other aspects of key pair management

6.3.1 Public key archiving

The CA's public keys are archived for 3 years after they have been used.

6.3.2 Key pair and certificate life spans

The **OTU CA** may not issue Holder certificates whose life spans exceed that of its own certificate; see section 5.6.

- Key pairs and one-time-use certificates have a life span of 15 minutes.
- Organisation certificates have a life span of 3 years.
- The CA's **expiry date** is **31/12/2020**.

6.3.3 Key inventory

The CA makes an inventory to make sure that all the private keys produced by the CA for the certificate Holder mechanism were requested properly.

6.3.4 Key pair destruction

Key pairs are destroyed in the following cases:

- The certificate has expired.
- The certificate associated with the key pair has been revoked.
- The key pair has expired.
- The CA has expired.

The destruction of the CA's private keys in the HSM requires that the keys contained in it be destroyed using the HSM's specific wiping functions so no information can be used to restore even part of these private keys.
All the backup copies of the CA's private keys must be destroyed in such a way that no information can be used to restore even part of these private keys. If the functions needed to destroy the CA's keys are inaccessible, or no longer accessible, in the HSM, then the latter must be destroyed physically.

These operations are carried out during an audited, Key Ceremony-type procedure.

6.4 Activation data

6.4.1 Activation data generation and installation

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

The activation data of the private keys of the **OTU's** CAs are generated during key ceremonies (see subsection 5.2.1 and the key ceremony document). These activation data are only known by the managers identified by name as part of the roles that were assigned to them (see subsection 5.2.1 and the key ceremony document).

6.4.1.2 Generation and installation of the activation data corresponding to the private key of the Holder certificate

The private keys of the Holder's certificate are generated by the certificate Holder mechanism. They are protected from use by a third-party through the use of HSMs certified in accordance with the FIPS 140-2 specification, level 2 or higher, for key generation and storage.

6.4.2 Activation data protection

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

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

6.4.2.2 Protection of the activation data corresponding to the private keys of Holder certificates

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

6.4.3 Other aspects pertaining to activation data

Not applicable

6.5 IT systems security mechanisms

6.5.1 Technical security requirements specific to IT systems

The minimum technical security requirements implemented meet the following objectives:

- user identification and authentication for accessing the system;
- use session management (disconnection after idle time, file access restrictions according to roles and usernames);
- protection against computer viruses and all forms of malicious or unauthorised software; software updates;
- management of users' rights and accounts;
- protection of the network against any intrusion by an unauthorised person;
- protection of the network to ensure the confidentiality and integrity of the data transmitted through it;
- audit functions (non-repudiation, accountability, and nature of the actions performed).

Security mechanisms (with automatic alerts) and procedures for auditing system settings (particularly routing settings) are implemented.

6.5.2 Evaluation of IT systems

The IT systems provided for the OTU PKI are audited in accordance with [ETSI102042] specifications.

6.6 Security measures for systems throughout their life cycles

6.6.1 Security measures with regard to system development

The implementation, component system configuration, and any change or update, are documented and monitored.

6.6.2 Security management measures

Any change made to the system of a component of the **OTU** is logged. It is documented and appears in the internal functioning procedures of the component concerned.

6.6.3 Evaluation of the security of systems' life cycles

Not applicable

6.7 Network security measures

The **OTU CA** is not in direct contact with open networks. Access gateways are protected against intrusion or attack attempts. These gateways restrict open services and protocols to the services that are essential for the **OTU** to function. These gateways are regularly updated to take into account the changes in anti-intrusion systems and to fix potential security holes as soon as they are identified by the community of network users. The components of the local network are maintained in a physically secure environment, and their configurations are periodically audited so they remain compliant with the requirements specified by the CA.

6.8 Timestamping system

The **OTU CA** does not use timestamping. The system time of the **OTU** PKI servers is used to date events. The clocks of the **OTU**'s systems are synchronised with one another using a reliable UTC time source.

7 Certificate, OCSP and CRL profiles

7.1 Certificate profiles

The certificates issued by the **OTU CA** contain the following fields:

- **Version**: X.509 (v3) certificate version,
- **Serial number**: serial number of the certificate (value unique to each issued certificate),
- **Signature**: OID of the algorithm used by the **OTU CA** to sign the CR,
- **Issuer**: value of the DN (X.500) of the CA that issues the certificate,
- **Validity**: activation and expiry dates of the certificate,
- **Subject:** value of the DN (X.500),
- **Subject Public Key Info:** OID of the algorithm and value of the public key,
- **Extensions**: extension list.

All these fields are signed with the **OTU CA**'s private key. Two fields are used for this signature:

- **Signature**: OID of the algorithm used, and
- **Signature Value**: result of the signature.

7.1.1 Version number

Holder certificates are X509 v3 certificates.

7.1.2 Certificate extensions

The extension can be critical or not. If the extension is critical, the user application which the certificate is submitted to must be able to handle this extension in accordance with its use. Otherwise i.e. the application cannot handle this extension or if the extension does not match the use expected by the application, the latter must reject the certificate

If the extension is not critical, the certificate is not rejected. In this case, the application is allowed to ignore the extension.

7.1.2.1 OTU CA's certificate

Basic field	**Value**
Version	2 (=version 3)
Serial number	Defined during the KC
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU 0002 378901946 (Worldline's SIREN number) CN = **AC Racine - Root CA - 2012**
Validity	Expires on 31/12/2020
Subject	C = FR O = Atos Worldline OU 0002 378901946 (Worldline's SIREN number) CN = **OTU CA**
Subject Public Key Info	rsaEncryption
Key size	2,048 bits
Extensions	**Value**
Authority Key Identifier (non-critical)	Identifier of the Root CA's public key
Subject Key Identifier (non-critical)	Identifier of the **OTU CA**'s public key. This identifier is defined by the root CA.
Key usage (critical): Definition of the use of the key	Signing of the certificate Signing of the certificate revocation list (Hexadecimal value: 0x06)
Certificate Policies (non-critical)	1.2.250.1.111.12.4.1 (OID of **AC Racine - Root CA - 2012**)
CPS URI (non-critical)	www.mediacert.com
User Notice Text (non-critical)	Conformance claim: 0.4.0.2042.1.3 ETSI 102 042 LCP level
Basic Constraints (critical)	Certification Authority Maximum depth: 0
CRL Distribution Points (non-critical)	http://root.mediacert.com/LatestCRL

7.1.2.2 One-time-use certificates

Basic field	Value
Version	3 (=version 4)
Serial number	Defined by the CA (unique)
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Worldline's SIREN number) CN = **OTU CA**
Validity	15 minutes
Subject	CN = Title [space] Forename [space] Subject's name [space] [TraceID] (1) O = OTU OU = Atos Worldline OU = Subscriber's name serialNumber = ReqTime - DocId – ClientID (2) C = FR
Subject Public Key Info	rsaEncryption
Key size	2,048 bits
Extension	**Value**
Subject alt name (non-critical)	RFC822 name: certificate Subject's e-mail address (3)
Authority Key Identifier (non-critical)	Identifier of the **OTU CA**'s public key
Subject Key Identifier (non-critical)	Identifier of the public key of the certificate. This identifier is defined by the OTU CA.
Key usage (critical)	nonRepudiation
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2.1** **URL: www.mediacert.com**
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2** **CP OID**
CPS URI (non-critical)	www.mediacert.com
Basic Constraints (non-critical)	Final entity
CRL Distribution Points (non-critical)	http://otu.mediacert.com/LatestCRL

(1)
TraceID represents the unique identification of the trace container for the signature.

(2)
In accordance with RFC 3739, the SerialNumber field in the DN makes it possible to eliminate the risk of homonymy in the rest of the DN fields. It is built as follows:

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

ReqTime is useful for the case where two people bearing the same name sign a document jointly.

The concatenation of these three pieces of information guarantees a unique value among all users.
This field can contain 128 characters at most.

(3) The **Subject alt name** field is optional and might not appear.

7.1.2.3 Organisation certificate

Basic field	Value
Version	3 (=version 4)
Serial number	Defined by the CA (unique)
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Worldline's SIREN number) CN = **OTU CA**
Validity	3 years
Subject	CN = Organisation's name OU = Name of the unit in the Organisation (optional)[1]1] OU = Subscriber's name OU = 0002 number under which the Organisation is registered in the country GN = Forename of the authorised individual in the Organisation (optional)[1] SN = Surname of the authorised individual in the Organisation (optional)[1] C = Organisation's country
Subject Public Key Info	rsaEncryption
Key size	2,048 bits
Extension	**Value**
Subject alt name (non-critical)	RFC822 name: Organisation representative's e-mail address
Authority Key Identifier (non-critical)	Identifier of the **OTU CA**'s public key
Subject Key Identifier (non-critical)	Identifier of the public key of the certificate. This identifier it is defined by the **OTU CA**.
Key usage (critical)	nonRepudiation, digital signature
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2.2** **URL: www.mediacert.com**
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2** **CP OID**
CPS URI (non-critical)	www.mediacert.com
Basic Constraints (non-critical)	Final entity
CRL Distribution Points (non-critical)	http://otu.mediacert.com/LatestCRL

[1] At least one of these two pieces of information must be present in the "Subject "field: the name of the unit in the Organisation, or the forename and surname of the authorised individual in the Organisation.

7.1.2.4 One-time-use certificate for test purposes

Basic field	Value
Version	1
Serial number	Defined by the CA (unique)
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Worldline's SIREN number) CN = **OTU CA**
Validity	15 minutes
Subject	CN = TEST title [space] Forename [space] Subject's name [space] [TraceID] (1) O = OTU OU = Atos Worldline OU = Subscriber's name serialNumber = ReqTime - DocId – ClientID (2) C = FR
Subject Public Key Info	rsaEncryption
Key size	2,048 bits
Extension	**Value**
Subject alt name (non-critical)	RFC822 name: certificate Subject's e-mail address (3)
Authority Key Identifier (non-critical)	Identifier of the **OTU CA**'s public key
Subject Key Identifier (non-critical)	Identifier of the public key of the certificate. This identifier is defined by the OTU CA.
Key usage (critical)	nonRepudiation
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2.3** **URL: www.mediacert.com**
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2** **CP OID**
CPS URI (non-critical)	www.mediacert.com
Basic Constraints (non-critical)	Final entity
CRL Distribution Points (non-critical)	http://otu.mediacert.com/LatestCRL

(3)
TraceID represents the unique identification of the trace container for the signature.

(4)
In accordance with RFC 3739, the SerialNumber field in the DN makes it possible to eliminate the risk of homonymy in the rest of the DN fields. It is built as follows:

- **ReqTime** represents the time at which the certificate was requested.
- **DocId** represents the ID of the document to sign (if several documents must be signed, the first document referenced in the signing request is used.).
- **ClientId** represents the unique ID of the client.

The concatenation of these three pieces of information guarantees a unique value among all users.
This field can contain 128 characters at most.

(3) The **Subject alt name** field is optional and might not appear.

7.1.2.5 Organisation certificate for test purposes

Basic field	Value
Version	1
Serial number	Defined by the CA (unique)
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Worldline's SIREN number) CN = **OTU CA**
Validity	3 years
Subject	CN = TESTOrganisation's name OU = Name of the unit in the Organisation (optional)[1]1] OU = Subscriber's name OU = 0002 number under which the Organisation is registered in the country GN = Forename of the authorised individual in the Organisation (optional)1 SN = Surname of the authorised individual in the Organisation (optional)1 C = Organisation's country
Subject Public Key Info	rsaEncryption
Key size	2,048 bits
Extension	**Value**
Subject alt name (non-critical)	RFC822 name: Organisation representative's e-mail address
Authority Key Identifier (non-critical)	Identifier of the **OTU CA**'s public key
Subject Key Identifier (non-critical)	Identifier of the public key of the certificate. This identifier it is defined by the OTU CA.
Key usage (critical)	nonRepudiation, digital signature
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2.4** **URL: www.mediacert.com**
Certificate Policies (non-critical)	**1.2.250.1.111.12.7.2** **CP OID**
CPS URI (non-critical)	www.mediacert.com
Basic Constraints (non-critical)	Final entity
CRL Distribution Points (non-critical)	http://otu.mediacert.com/LatestCRL

[1] At least one of these two pieces of information must be present in the "Subject" field: the name of the unit in the Organisation, or the forename and surname of the authorised individual in the Organisation.

7.1.3 Algorithm OID

The algorithm used is sha256WithRSAEncryption. Its OID is: 1.2.840.113549.1.1.11.

7.1.4 Naming schemes

Names comply with the requirements set out in section 3.1.

7.1.5 Naming constraints

The “CommonName” attribute (CN) of an OTU certificate and—should the case arise—the “GivenName” (GN) and “SurName” (SN) attributes of an Organisation certificate contain the first forename of the Subject’s personal information. This CP does not impose any requirement with regard to forenames apart from the usual first forename.
The hyphen is used as separator for compound forenames and names.
The "serialNumber" attribute present on the certificates is used to handle homonymy cases.

The title contains:

- “Mr.” for a male user, or
- “Ms” for a female user.

Example:

- Jean François MARTIN DUPONT => commonName = Jean-François MARTIN-DUPONT M

7.1.6 CP OID

See subsection 1.2.2.

7.1.7 Use of the "policy constraints" extension

This CP formulates no requirements in this regard.

7.2 CRL profile

7.2.1 CRLs and extensions

The CRLs issued by the **OTU** contain the following fields:

- **Version**: CRL version (v2),
- **Signature**: OID of the algorithm used by the **OTU** to sign the CRL,
- **Issuer**: value of the DN (X.500) of the CA that issues the CRL,
- **This Update**: date on which this CRL update was generated,
- **Next Update**: date on which the next CRL update will be generated,
- **Revoked Certificates**: list of the revoked certificates with their serial numbers and revocation dates, and
- **Extensions**: extension list.

All these fields are signed with the **OTU CA**’s private key. Two fields are used for this signature:

- **Signature**: OID of the algorithm used, and
- **Signature Value**: result of the signature.

The extensions used are **Authority Key Identifier** and **CRL Number**. The CRL is valid for 7 days. CRLs are published every 24 hours.

Basic field	**Value**
Version	1 (=version 2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Worldline's SIREN number) CN = OTU CA
This Update	
Next Update	This Update + 7 days
Revoked Certificates	List of the revoked certificates: • userCertificate • revocationDate • reason for the revocation
Extension	**Value**
Authority Key Identifier (non-critical)	Identifier of the **OTU CA**'s public key
CRL Number (non-critical)	Number of the CRL defined by the **OTU CA**

7.3 OCSP profile

The **OTU CA** does not implement any OSCP-type services.

8 Compliance audit and other evaluations

The CA's compliance with the requirements of this CP is evaluated by an audit firm that has been authorised to evaluate the CA in accordance with the technical specifications produced by [ETSI102042]. The certification is granted by COFRAC (*French accreditation committee*).

The rest of this chapter only concerns the audits and evaluation of the elements which the CA is responsible for.

8.1 Frequency and circumstances of audits

The CA has compliance verified once a year.

In the case of an important change, the CA can request an early compliance verification.

8.2 Auditors' identities and qualifications

Components are audited by a team of auditors who are allowed to audit the **OTU CA** and have the required authorisations to carry out audits in accordance with [ETSI102042] specifications.

8.3 Relationships between auditors and audited entities

The (duly authorised) audit team is different from the team that manages the **OTU CA.**

8.4 Subjects covered by audits

The verifications carried out by the duly authorised auditors concern the entire CA. The objective is to make sure that this CP, the associated CPS, and all the elements that derive from them (operational procedures, implemented resources, etc.) are complied with.

8.5 Actions carried out following audit conclusions

The Audit team gives its opinion to the CA operation manager. An audit can have three possible results: Passed / To be confirmed / Failed.

8.5.1 Passed

If no instances of non-compliance have been detected, the operation manager confirms the compliance to the audited component of the audited **OTU CA**.

8.5.2 To be confirmed

If minor nonconformities have been detected, the CA's Operation Manager informs the audited component about the nonconformities that must be fixed and the deadline for doing so. A later confirmation inspection is carried out to get rid of the critical nonconformities that have been detected.

8.5.3 Failed

If the audit fails, and depending on the nonconformities that have been detected, the auditors recommend the following actions to the CA:

- temporary or definitive cessation of activity,
- revocation of the certificate of the audited component,
- revocation of all the certificates that have been issued since the last positive verification, or

- revocation of the CA's certificate.

Worldline will decide on the measure that will be taken.

8.6 Publication of results

The results of these compliance verifications are published at www.mediacert.com in the form of an up-to-date certification document.

9 Other business and legal issues

9.1 Prices

The **OTU CA** does not market its certificates alone, but only through higher-level services.

9.2 Insurance

9.2.1 Insurance coverage

Worldline has insurance coverage against the risks for which it might be held liable.

9.2.2 Other resources

This CP formulates no specific requirements in this regard.

9.2.3 Coverage and guarantee applicable to user entities

This CP formulates no specific requirements in this regard.

9.3 Professional data confidentiality

9.3.1 Scope of secret information

Only Secret Holders have access to secret data e.g. the information pertaining to the security of the PKI, such as the activation data and private keys of the CA and its Operators.

9.3.2 Scope of confidential information

The following information is considered as confidential:

- the technical information pertaining to the security of the inner workings of the PKI's cryptographic modules and components;
- CA event logs;
- technical intervention follow-up information;
- the CPS and internal operation procedures;
- audit reports.

Only the people that have been authorised by Worldline and need to know or be granted access to this confidential information may view it on demand.

The authorisation is granted by the application manager of the OTU PKI.

9.3.3 Non-confidential information

The **OTU CA's** non-confidential information is public and can be accessed at www.mediacert.com

The information that falls out of the scope of confidential information is considered as "Internal document" or "Limited circulation" in accordance with the levels described in Worldline's ISSP.

9.3.4 Responsibilities with regard to the protection of confidential information

The CPS specifies the security procedures that guarantee the confidentiality of the information defined as confidential in subsection 9.3.1. In particular, it describes the methods used for the permanent deletion or the destruction of the media used to store such information.

The CA complies with the laws and regulations in force on the French territory. In particular, it may have to make Registration files available to third parties as part of legal procedures. It also gives certificate Subjects access to this information.

9.4 Protection of personal data

9.4.1 Personal data protection policy

In accordance with the regulations in force, notably the French "Data Protection Act", the Certification Authority sees to the protection of the personal data that are or are likely to be in its possession.

Act n° 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, amended by Act n° 2004-801 of 6 August 2004 relative to the protection of individuals with regard to the processing of personal data, is applicable to all the documents kept or sent by the CA or a component of the PKI (website of the French Data Protection Authority: http://www.cnil.fr).

As per the law, natural people have the right to access, rectify or oppose the use of the personal information that concerns them and which the **OTU CA** has in its possession. The contact of the **OTU CA** is the person to contact for this right to be exercised.

9.4.2 Personal Information

The information that is considered as personal includes the registration data of the Subject or authorised individuals as supplied by the Subscriber.

9.4.3 Non-personal information

This CP formulates no specific requirements in this regard.

9.4.4 Responsibilities with regard to the protection of personal data

The CA acts in accordance with the laws and regulations in force on the French territory.

9.4.5 Use of personal data - Notification and consent

The information which the Subscriber entrusts the CA with is protected against disclosure without the Subscriber's consent. The CA acts in accordance with the laws and regulations in force on the French territory.

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

The CA acts in accordance with the laws and regulations in force on the French territory.

9.4.7 Other circumstances under which personal information is disclosed

This CP formulates no specific requirements in this regard.

9.5 Intellectual and industrial property rights

The laws and regulations in force on the French territory are applicable.
Public documents, which fall outside the scope of confidential information, remain the property of Worldline.

9.6 Obligations and Guarantees

The CA must make sure that

- the private key is protected (integrity and confidentiality) during its generation and throughout the validity periods of the key and activation data;
- key pairs and certificates are used only for the uses defined in section 4.5 in accordance with commitments.
- the CPS is implemented and complied with.
- it will subject itself to the compliance verifications carried out by external auditors, and will implement their recommendations;
- the technical and human resources needed to honour commitments will be implemented, notably with regard to the specified service level;
- its policies and procedures do not contain any discriminatory practices;
- internal functioning procedures are documented.

9.6.1 Certification Authority

The CA must

- guarantee and maintain the consistency between its CPS and its CP,
- ensure that the RA complies with the CP and the CPS;
- work with auditors during compliance verifications and when implementing the measures that may have been decided upon with these auditors following these verifications.

9.6.2 Registration Authority

The RA must comply with the Registration procedures described in this CP and the CPS.

9.6.3 Subjects' obligations

Certificate Holders must

- protect the access to private keys and certificates,
- only use their certificates for the uses provided for in the associated CP,
- revoke their certificate or have it revoked if its compromised or suspected of being compromised,
- comply with the CP and CPS requirements that are applicable to them.

9.6.4 Subscribers

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

- collect the identity information given by the Subject;
- verify the identity information given by the Subject;

- inform the Subject of their obligations; see subsection 9.6.5;
- send the Subject's identification data in its request;
- draw up and sign the Subject's certificate request;
- keep exclusive control over the methods is uses to authenticate itself with the **OTU CA**;
- inform the **OTU CA** as early as possible of any event that might be detrimental quality of the identification of its Subjects;
- inform the **OTU CA** as early as possible of any event that might be detrimental to the reliability of its authentication methods;
- inform the Subject about the certificate request process and the consequences of using the certificate (electronic signature) in accordance with this CP.

For an Organisation certificate, the Subscriber must

- complete the certificate request file by supplying all the required elements, and the necessary supporting documents and proxies. The Organisation can be identified by means of its SIREN number, company registration certificate, statutes or any other valid legal document that is appropriate to the Organisation's form and statutes.
- inform the CA if the certificate becomes invalid because of a change in the Organisation. To do so, the Organisation must send the following information to the RA immediately by means of registered mail with acknowledgement of receipt:
    - Any change in the identity of the person who holds the role of Subscriber representative or deputy Subscriber representative, the effective date of this change and the supporting documents.
    - Any change in the information sent to the RA and the effective date of these changes.
- request the revocation of the certificate in the situations listed in the CP. In this regard, the change in the information appearing on an Organisation Certificate entails the revocation of the Certificate and its replacement at the Organisation's expense.
- inform the **OTU CA** immediately of any event that might be detrimental to the reliability of its authentication methods. To do so, the changes (name, forename, e-mail address) must be notified; and
- inform the CA should the Organisation no longer exist. In this regard, Organisation's Subscriber representative must report all the changes affecting all Organisation certificates (change in the name, postal address, e-mail address or SIREN number of the Company) and send the supporting documents by means of registered mail with acknowledgement or receipt.

The changes made to information that does not appear on the Certificate do not affect its validity. They are notified via ordinary mail.

If the Subscriber resorts to a technical service provider, it is the Subscriber's responsibility to make the latter comply with these obligations.

Besides, this provider may hold secrets that are specific to the Subscriber, such as private keys associated with to authentication and message signing certificates. It is the Subscriber's responsibility to make sure that access to these secrets is actually protected by appropriate measures.

9.6.5 Subject

The future Subject of a certificate must give the Subscriber information and supporting documents that are accurate and up to date at the date on which the certificate is requested.

9.6.6 Certificate users

Certificate users (third-party people or application) must

- verify the use for which a certificate has been issued, and comply with it,
- verify the validity of the certificate (not expired, not revoked, integrity), and

- verify the validity of each certificate of the certification chain.

9.6.7 Other participants

Not applicable

9.7 Limited guarantee

Through its services, the **OTU CA** guarantees:

- the authentication of the Subscriber by the CA through the Subscriber's certificate;
- the generation of certificates in accordance with the request of a Subscriber authenticated beforehand;
- the provision of the certificate validity information in accordance with this CP.
- the exclusive control of the private key by the certificate Holder mechanism, and the destruction of this key after a one-time-use session (case of one-time-use certificates).

No other guarantee is provided.

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

- use of an expired certificate,
- use of a revoked certificate, or
- use of a certificate for a use other than those described in section 4.5 of this CP.

The CA undertakes to issue the certificates in accordance with this CP and the state of the art.

9.8 Limited liability

The CA may only be held liable if it fails to meet its obligations.

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

- use of an expired certificate,
- use of a revoked certificate, or
- use of a certificate for a use other than those described in section 4.5 of this CP.

The CA undertakes to issue the certificates in accordance with this CP and the state of the art.

9.9 Compensation

The **OTU CA** delivers certificates as part of more complete electronic online subscription services.

The framework agreement signed between the Customer and Worldline or its duly authorised agent sets out the compensation. If there is no framework agreement, Worldline's General Terms of Sale will be applicable.

9.10 Validity period and early expiry of the CP

9.10.1 Validity period

The **OTU CA's** CP is effective only after it has been validated by the entity that manages the CP. The CP remains in force until the last certificate issued in accordance with it expires.

9.10.2 Early expiry

Compliance work due to a change in the CP does not affect the certificates that have already been issued.

9.10.3 Effects of expiry - Clauses that remain applicable

This CP formulates no specific requirements in this regard.

9.11 Individual notifications and communications between participants

Should a change affect this CP, the CA will have to inform Subscribers about it two months before the start of the operation, at the latest.

The CA will also inform Subscribers one month after the end of the operation, at the latest.

This CP does not formulate any requirements with regard to the validation of changes by Subscribers.

All the components and participants of the PKI are kept posted about the changes made to the CP and the impacts that these changes have on them.

9.12 Amendment procedures

The revisions of this CP are decided upon by the security committee that manages the CP. This CP is written by Worldline. Formatting changes (spelling...) are not subjected to validation, and the CP can be updated without any prior notifications.

The Security Committee is in charge of amending this CP. This Committee meets at least once a year to list the changes required to maintain compliance with the rules and standards in force. It notably consists of the following managers:

- the local Worldline ISO or a member of the same structure within Worldline,
- a CA representative, and
- the team in charge of monitoring the compliance of platforms.

9.12.1 Amendment process and information period

All the components and participants of the PKI are kept posted about the changes made to the CP and the impacts that these changes have on them.

9.12.2 Circumstances under which the OID must be changed

If the security committee thinks that a change to the CP or CPS has consequences on the security or trust in the CA, it may define a new certification policy with a new OID.

9.13 Dispute resolution clause

This CP is governed by French law. The writing and implementation of this CP comply with the state of the art, laws and regulations.

The framework agreement signed between the Customer and Worldline or its duly authorised agent sets out the clauses with regard to dispute resolution. If there is no framework agreement, Worldline's General Terms of Sale will be applicable.

Worldline's ISO is the authorised contact for any comment, request for additional information, claim or submission of a litigation file.

9.14 Jurisdiction

The laws and regulations in force on the French territory are applicable.

The framework agreement signed between the Customer and Worldline or its duly authorised sets out this clause. If there is no framework agreement, Worldline's General Terms of Sale will be applicable.

9.15 Compliance with laws and regulations

The laws and regulations in force on the French territory are applicable.

9.16 Miscellaneous clauses

9.16.1 Global agreement

This CP formulates no specific requirements in this regard.

9.16.2 Activity transfers

See section 5.8

9.16.3 Consequences of an invalid clause

This CP formulates no specific requirements in this regard.

9.16.4 Application and waiver

This CP formulates no specific requirements in this regard.

9.16.5 Force majeure

The concept of “force majeure” encompasses all the events that are usually recognised as such by French courts, notably irresistible, unsurmountable, unpredictable events. Therefore, the CA may not be held liable for any indirect damages and service interruptions resulting from force majeure.

The framework agreement signed between the Customer and Worldline or its duly authorised agent sets out this clause. If there is no framework agreement, Worldline's General Terms of Sale will be applicable.

9.17 Other clauses

This CP formulates no specific requirements in this regard.

10 Appendix

10.1 Regulation / Standardisation

Reference	Document
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework
[ETSI102 042]	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates V2.2.1 (2011-12)
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

10.2 Contractual document

Reference	Document
[DPC OTU]	Certificate Practice Statement of the OTU CA Reference: OTU DPC 0003 Version 1.0

10.3 Requirements with regard to security objectives

The cryptographic module (HSM) that the CA uses to generate and implement its signing keys (which are used to generate electronic certificates and CRLs) meets the following security requirements:

- It ensures the confidentiality and integrity of the CA's private signing keys throughout their life cycles, and guarantees their secure destruction at the end of their lives.
- It is capable of identifying and authenticating its users.
- It restricts access to its services according to the user and the role assigned to them.
- It is capable of running a series of tests to make sure that it works correctly, and entering a secure state if it detects an error.
- It makes it possible to create a secure electronic signature to sign the certificates generated by the CA; this signature that does not reveal the CA's private keys and cannot be forged without knowing the private keys.
- It creates audit records for each security-related change.
- If a function for backing up and restoring the CA's private keys is provided, it guarantees the confidentiality and integrity of the backed-up data and requires at least twofold verification of the backup and restoration operations.

10.4 Qualification requirements

The cryptographic module that the CA uses to generate, store and use the CA's keys has been granted a "reinforced level" qualification by the ANSSI (*French national agency in charge of the security of information systems*).

End of document