PUBLIC

ONLINE CAS GENERAL CONDITIONS OF SERVICES

AUTHOR(S)	:	F. Da Silva
DOCUMENT NO	:	WLS-OTU-F022
VERSION	:	2.3
STATUS	:	Final
SOURCE	:	Worldline
DATE OF THE DOCUMENT	:	December 23, 2019
NUMBER OF PAGES	:	12
OWNER	:	MediaCert Committee

TSP MediaCert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2020-01-14 17:18:30

Table of Contents

List of changes

Version	Date	Description	Author(s)
1.0	24/10/2014	Initial Public Version	J.J. Milhem
2.0	05/07/2017	Rewriting to take into account eIDAS regulatory constraints	F. Da Silva
2.1	18/09/2018	Correlation with the integration of CP-CPS into the documentary structure of Mediacert TSP. No modification(s) made other than the formatting of this document	F. Da Silva
2.2	18/09/2018	Adding a CA to the CP-CPS perimeter which implies upgrading these GCS. These CGS then become the CGS of the "online CA".	F. Da Silva
2.3	14/01/2020	Adding the certificate holders obligations.	F. Poulain

1 Introduction

1.1 Presentation of the document

This document defines the essential provisions defined in the [CP-CPS] concerning the issue of certificates by the so-called "online" Certification Authorities at the Subscriber's request, in accordance with the regulations [eIDAS] and more particularly [ETSI EN 319 411-1]. The online CAs operated by Mediacert TSP, itself established by Worldline, are as follows:

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

Unless otherwise stated, the requirements of this document are applicable to the above-noted CAs. Requirements applicable to a single CA are preceded by the statement:

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

It is specified, however, that because of its synthetic nature, this document does not replace the [CP-CPS] referred to in chapter 1.3.

It should be recalled that the issuance of certificates by these CAs is based on the establishment of a prior contractual relationship between an organization, which is then designated as Subscriber, and Worldline. The organization, now a Subscriber, then registers for the services delivered by Mediacert TSP to obtain the delivery, at its choice, of:

- single-use signature certificates, issued in the name of a natural person who has authorized it for this purpose, in order to be able to sign one or more documents in electronic form; and/or
- organization certificates, issued in the name of organizations which depend on the Subscriber or in the name of organizations which expressly mandate him for this purpose, in order to be able to seal one or more documents in electronic form.

Holders of certificates issued by online CAs must, prior to any use of their certificates, be aware of the terms of use of those certificates that are expressed in these General Conditions of Services and in the [CP-CPS].

Indeed, before using any certificate issued by one of these CAs, the user must read the [CP-CPS] available on the Mediacert TSP website at the following address: https://www.mediacert.com.

1.2 Acronyms

The acronyms used in this document are as follows:

Acronym	Description
CA	Certification Authority
GSC	General Subscription Conditions
GCS	General Conditions of Services
GCSS	General Conditions of Sale and Services

Acronym	Description
PKI	Public Key Management Infrastructure
LCP	*Lightweight Certificate Policy*
OID	*Object Identifier*
OTU	*One Time Usage*
CP-CPS	Certification Policy / Certification Practice Statement

1.3 References

The structure of this document is in accordance with Annex A2 -"*The PDS structure*" *of the* technical specification [ETSI EN 319 411-1].

1.3.1 Regulation

Reference	Description
[CNIL]	Law n°78-17 of 6 January 1978 relating to data processing, files and freedoms, amended by law n°2004-801 of 6 August 2004
[eIDAS]	REGULATION (EU) No 910 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[RGPD]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

1.3.2 Technical regulations

Reference	Description
[ETSI IN 319 411-1]	ETSI EN 319 411-1 v1.2.2 (2018-04) Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

1.3.3 Internal documentation

Reference	Description
[GSC]	General Subscription Conditions Online Certification Authorities Reference : WLS-OTU-F008
[GCSS]	General Conditions of Sale and Services Worldline Reference : 212007

Reference	Description
[CP-CPS]	Certification Policy - Certification Practice Statement Online Certification Authorities Reference : WLM-OTU-F002 OID : 1.2.250.1.111.20.5.3

2 General Conditions of Services

<table>
<tr><th>Type of information</th><th>Description</th></tr>
<tr><td>Point of contact</td><td>MediaCert Committee
Worldline
23 rue de la Pointe
Industrial Zone A
59113 Seclin
France
dl-mediacert-tsp@worldline.com</td></tr>
<tr><td>Certificate type, validation procedure and use</td><td>Online CAs produce six (6) certificate ranges:
<table>
<tr><th>Scope</th><th>Certificate Range</th><th>Compliance and Targeted Security Level</th><th>IDO</th></tr>
<tr><td rowspan="4">OTU CA</td><td>"Reinforced" single-use certificates</td><td>ETSI EN 319 411-1] LCP level (unqualified)</td><td>1.2.250.1.111.20.5.3.1</td></tr>
<tr><td>Organization Certificates</td><td>ETSI EN 319 411-1] LCP level (unqualified)</td><td>1.2.250.1.111.20.5.3.2</td></tr>
<tr><td>"Reinforced" single-use test certificates</td><td>ETSI EN 319 411-1] LCP level (unqualified)</td><td>1.2.250.1.111.20.5.3.3</td></tr>
<tr><td>Test Organization Certificates</td><td>ETSI EN 319 411-1] LCP level (unqualified)</td><td>1.2.250.1.111.20.5.3.4</td></tr>
<tr><td rowspan="2">LCP OTU CA</td><td>"Standard" single-use certificates</td><td>ETSI EN 319 411-1] LCP level (unqualified)</td><td>1.2.250.1.111.20.5.3.5</td></tr>
<tr><td>"Standard" single-use test certificates</td><td>ETSI EN 319 411-1] LCP level (unqualified)</td><td>1.2.250.1.111.20.5.3.6</td></tr>
</table>
A single-use certificate is dynamically produced at the Subscriber's request on behalf of a natural person (Holder) at the Subscriber's request during the electronic signature process. The [CP-CPS] further specifies that:
• [OTU LCP] the identity of the future Holder may be checked automatically in order to verify the declared identity of the</td></tr>
</table>

Type of information	Description
	Holder; • [OTU] the identity checks of the future Holder must be carried out by operators in order to be able to verify the Holder's identity in a physical manner. [OTU] The organization certificate is produced by the OTU CA at the request of the Subscriber on behalf of an organization for which the Subscriber is entitled to request a document seal. Test certificates are issued for: • technical uses; • demonstrations; • acceptance tests of changes made to the production information system; on request of: • a Subscriber; • Worldline; on behalf of: • a natural person (Holder) ; • an organization; • Worldline. Certificate recovery : • When sending the signed contract in PDF, the signatory can retrieve his certificate by double clicking on his signature. • Thus the "Signature Validation Status" window opens, and the signatory must click on "Signature Properties ..." • Finally click on "Show Certificate" The certificate then appears. These certificates cannot be used in other contexts. A set of actions and means is put in place, during the registration procedure, to identify the applicants and future Holders of certificates and validate the information present within the issued certificates (cf. chapter 3.2 of the [CP-CPS]).

<table>
<tr><th>Type of information</th><th>Description</th></tr>
<tr><td></td><td>The acceptance conditions of certificates are as follows:

<table><tr><th>Certificate Type</th><th>Conditions of acceptance</th></tr><tr><td>Single-use certificate</td><td>The explicit acceptance of the data contained in the certificate by the future Holder is made prior to its issuance.</td></tr><tr><td>[OTU] Certificate of organization</td><td>The explicit acceptance of the data contained in the certificate either by the legal or statutory representative of the Subscriber who made the request, or by the authorized individual identified in the certificate is made within ten (10) working days following the generation of the concerned certificate by e-mail. Once this period has expired, the certificate is deemed to conform.</td></tr></table></td></tr>
<tr><td>Limitations on the use of certificates</td><td>Product certificates may only be used for subscription or dematerialized transmission procedures, in order to:

• electronically sign a static electronic document in PDF format with a single-use certificate;

• [OTU] electronically seal a static electronic document in PDF format with an organization certificate.

The archived data are defined in chapter 5.5.1 of the [CP-CPS].

The period for which these data are kept depends on the data in question. The retention period of the registration file archives for a single-use certificate is eight (8) years. The retention period for registration records for a certificate of organization is ten (10) years. This is consistent with the obligations incumbent on certification service providers.
More details defined in chapter 5.5.2 of the [CP-CPS].</td></tr>
<tr><td>Obligations of certificate holders.</td><td>The holders of certificates have the obligation to:

• protect the means of access to private keys and certificates;

• use their certificates only for the purposes intended and defined in the associated [CP-CPS];

• revoke or request revocation of their certificate in the event of compromise or suspected compromise;

• revoke or request the revocation of their certificate in the event of compromise or suspicion of compromise of the means of access;

• revoke or request the revocation of their certificate if it contains information that has become obsolete;</td></tr>
</table>

Type of information	Description
	• No longer use their private key in the event of compromise or suspected compromise; • verify and comply with their obligations as described in this document and in the [CP-CPS] and, in the case of single-use certificates, in the contract with their agent, here referred to as the Subscriber. Before placing their trust in the said certificate, the certificate holder must imperatively verify its validity with the TSP MediaCert by consulting the most recent and appropriate Revoked Certificates Lists, as well as by verifying its validity, in particular its expiration date and its signature, and the validity of the certificate. Failing to fulfill this obligation, the certificate holder alone assumes all the risks of his actions which do not comply with the requirements of the [CP-CPS], the TSP MediaCert therefore no longer guarantee any legal value for the certificates it has issued and that could have been revoked or that would not be valid. In addition, the future Holder is obliged to provide information and supporting documents requested by the Subscriber, which he certifies as accurate and up-to-date when applying for the certificate. The obligations incumbent upon the future Holder are also defined in the contract concluded with his representative, here referred to as the Subscriber. The **Subscriber's** specific obligations, which are in addition to those listed above, are defined in chapter 9.6.3.1 of the [CP-CPS] as well as in the [GSC] he has signed with Worldline.
Obligations of certificate users	Users of certificates generated by online CAs are required to: • verify and comply with their obligations under the [CP-CPS] and these General Conditions of Services. These obligations will be for single-use certificates described by the Subscriber in the contract binding him to the future Holder. This contract explains the operation of a signature in electronic form, the implications of this choice, the procedures for obtaining the necessary consents in accordance with those contained in its Subscription Contract; • verify and respect the use for which a certificate has been issued; • verify the validity of the certificate (expiration, revocation, integrity) and that of each certificate in the certification chain.
Requirements for verification of certificate status by users	In the context of the use of a single-use certificate provided by one of the online CAs, the [CP-CPS] do not, in view of the atomic nature of the signature operation, make any requirement regarding the obligation to verify the revocation of the certificate. [OTU] When using a certificate of organization provided by the OTU CA,

Type of information	Description
	the user shall verify the status of the certificate on which he intends to rely before using it. For this, he can use the various information services made available by the OTU CA. In addition to the status, the user must check the validity of the certificate in question and the corresponding certification chain.
Limitations of warranties and liabilities	The online CAs undertake to issue certificates in accordance with the [CP-CPS] and the state of the art. Mediacert TSP guarantees through its services: • the Subscriber's authentication with his certificate by the Registration Authority; • the generation of certificate(s) in accordance with the Subscriber's request, previously authenticated and verified; • the provision of information functions on the status of certificates issued, following the Subscriber's request, by CAs in accordance with this document; • the exclusive control of the private key of the certificate by the Certificate Carrying Device and the destruction of this same key after a single session of use in the case of a single-use certificate. No other warranty is provided. Mediacert TSP can only be held liable in the event of proven non-compliance with its obligations. The Mediacert TSP cannot be held liable in the event of a fault within the scope of a Subscriber entity, in particular in the event of: • use of an expired certificate; • use of a revoked certificate; • use of a certificate in an application other than those described in the *"Certificate Usage Limitations"* section of this document. The CAs are generally not responsible for the documents and information transmitted by the Subscriber and do not guarantee their accuracy or the consequences of damaging facts, actions, negligence or omissions by the Subscriber, his representative or the Holder. The Subscriber undertakes not to make any commitment in the name and on behalf of the CAs for which it can under no circumstances substitute itself.
Applicable references	The applicable references are defined in chapter 1.3 of this document. Online CAs documentation is available on MediaCert TSP website at https://www.mediacert.com.

Type of information	Description
Privacy Policy	Worldline takes all necessary measures to ensure the confidentiality of professional (cf. chapter 9.3 of the [CP-CPS]) and personal (cf. chapter 9.4 of the [CP-CPS]) data in accordance with French legislation in force on French territory.
Compensation policy	The issuance of certificates by the CAs concerned by this document is carried out within the framework of higher level services such as electronic subscription. The framework agreement signed between the Subscriber and Worldline, or its duly authorized agent, specifies the conditions for compensation in the event of damage. In the absence of a framework agreement, Worldline's [GCSS] will apply.
Applicable law	The online PKIs in all their components and including documentaries are governed by the legislation and regulations in force on French territory applicable to them, although their activities arising from the [CP-CPS] may have legal effects outside French territory. The framework agreement signed between the customer and Worldline, or its duly authorized representative, specifies the provisions concerning dispute resolution. In the absence of a framework agreement, Worldline's [GCSS] will apply. The authorized contact for any comment, request for additional information, complaint or dispute file regarding the [CP-CPS] is defined in the *"Point of contact"* section of this document.
HQ Audits	Worldline regularly carries out an external audit of certification to the [ETSI EN 319 411-1] standard for its online CAs by an independent and accredited body.