Document reference	OTU.CG.0022
Document revision:	2.0
Document date:	7/5/2017
Classification:	Public

OUT Certification Authority

Terms of Service

Changelog

Version	Date	Author	Reason
1.0	10/24/2014	J.J. Milhem	Initial public release
2.0	7/5/2017	F. Da Silva	Rewriting to take into account eIDAS regulatory constraints

CYRIL LOOTVOET

Signature numérique de CYRIL LOOTVOET
Date : 2018.04.12 14:31:23 +02'00'

1 Introduction

1.1 Presentation of the document

This document defines the essential provisions defined in the CP-CPS concerning the issuance of certificates by the OTU Certification Authority at the Subscriber's request, in accordance with the EIDAS regulation and more particularly with [ETSI EN 319 411-1] .

However, it must be noted that because of its synoptic nature, this document does not replace the CP-CPS referenced in section 1.3.

It should be recalled that the issuance of certificates by the OTU CA is based on the establishment of a prior contractual relationship between an organization, which is then referred to as the Subscriber, and Worldline. The organization, now a Subscriber, then subscribes to the services delivered by the OTU CA to obtain the delivery, as it chooses, of:

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

Before using them, the Subjects of the certificates issued by the OTU CA must read the conditions of use of these certificates, which are set out in these Terms of Service and in the CP-CPS.

Indeed, before any use of a certificate issued by the OTU CA, the user must read the CP-CPS available on the OTU CA's website at https://www.mediacert.com

1.2 Acronyms

The following acronyms are used in this document:

Acronym	Description
CA	Certification Authority
CP-CPS	Certification Policy - Certification Practice Statement
GTOS	General Terms of Subscription
GTS	General Terms of Sales
LCP	Lightweight Certificate Policy
OID	Object Identifier
OTU	One-Time-Use
PKI	Private Key Infrastructure
TOS	Terms of Service

1.3 References

The structure of this document complies with “Annex A2 - The PDS structure” of technical specification [ETSI EN 319 411-1].

TECHNICAL REGULATIONS	
Reference	**Description**
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

REGULATIONS	
Reference	**Description**
[CNIL]	Act No. 78-17 of January 6, 1978 on information technology, data files and civil liberties amended by act No. 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 trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC

TECHNICAL DOCUMENTATION OF THE OTU PKI	
Reference	**Description**
[OTU CG 0008]	General Terms of Subscription OTU Certification Authority Reference: OTU CG 0008
[212007]	General Terms of Sale and Services Worldline Reference: 212007
[OTU PC-DPC 0002]	Certification Policy / Certification Practice Statement OTU Certification Authority Reference: OTU PC-DPC 0002

2 Terms of Service

<table>
<tr><th>Type of information</th><th>Description</th></tr>
<tr><td>Point of contact</td><td>Comité "MediaCert OTU"
Worldline
1, rue de la Pointe
Zone Industrielle A
59113 Seclin
France
dlfr-mediacert-ac-otu@atos.net</td></tr>
<tr><td>Type of certificate, validation procedure and use</td><td>
The OTU CA produces four (4) types of certificates:
<table>
<tr><th>Type</th><th>OID</th><th>Conformity</th><th>Security level</th></tr>
<tr><td>one-time-use</td><td>1.2.250.1.111.17.0.3.1</td><td>[ETSI EN 319 411-1]</td><td>LCP</td></tr>
<tr><td>organization</td><td>1.2.250.1.111.17.0.3.2</td><td>[ETSI EN 319 411-1]</td><td>LCP</td></tr>
<tr><td>one-time-use certificate for test purposes</td><td>1.2.250.1.111.17.0.3.3</td><td>[ETSI EN 319 411-1]</td><td>LCP</td></tr>
<tr><td>organization certificate for test purposes</td><td>1.2.250.1.111.17.0.3.4</td><td>[ETSI EN 319 411-1]</td><td>LCP</td></tr>
</table>
A one-time-use certificate is generated dynamically by the OTU CA at the Subscriber's request and on behalf of a natural person (Subject) during the electronic signature process.

The organization certificate is produced by the OTU CA at the Subscriber’s request and on behalf of an organization for which the Subscriber is authorized to request the sealing of documents.

Test certificates are issued for:
• technical purposes,
• demonstration purposes, and
• acceptance tests of changes made to the production information system.

at the request of:
• a Subscriber, or
• Worldline.

on behalf of:
• a natural person (Subject),
• an organization, or
• Worldline.

These certificates cannot be used in other contexts.

During the registration procedure, the OTU PKI implements actions and resources to identify the requisitioners and future Subjects of certificates, and to validate the information contained in the certificates issued (see section 3.2 of the CP-CPS).
</td></tr>
</table>

Type of information	Description
Restrictions on the use of certificates	The certificates produced can only be used as part of a dematerialized subscription or transmission procedure in order to: • electronically sign an electronic static document in PDF format with a one-time-use certificate, and • electronically seal an electronic static document in PDF format with an organization certificate. The archived data are defined in subsection 5.5.1 of the CP-CPS. The retention period of these data depends on the latter. The retention period for registration file archives for one-time-use certificates is eight (8) years. The retention period for registration file archives for organization certificates is ten (10) years. Further details can be found in subsection 5.5.2 of the CP-CPS.
Certificate beneficiaries' obligations	Certificate beneficiaries shall: • protect the means of access to private keys and certificates; • only use their certificates for the uses provided for in the associated CP-CPS; • revoke their certificate or have it revoked if it is compromised or suspected of being compromised; • revoke or request the revocation of their certificate if the means of access are compromised or suspected of being compromised; and • verify and meet their obligations as described in this document and in the CP-CPS; and, in the case of one-time-use certificates, in the contract signed with their agent, hereafter referred to as the Subscriber. When requesting a certificate, the future subject thereof must give the Subscriber information and supporting documents that are certified as accurate and up to date. The obligations incumbent on the future subject are also defined in the contract signed with their agent, hereafter referred to as the Subscriber. The Subscriber's specific obligations are defined in paragraph 9.6.3.1 of the CP-CPS as well as in the GTOS that it signed with Worldline.
Certificate users' obligations	The users of the certificates provided by the OTU CA must • verify and meet the obligations incumbent upon them in the CP-CPS and in the Terms of Service. For one-time-use Certificates, these obligations will be described by the Subscriber in the contract that binds it with the future Subject. This contract sets out the functioning of an electronic signature, the implications of this choice, and the procedures for executing it with the necessary consent collection operations in accordance with those contained in the aforementioned Subscription Contract. • verify the use for which a certificate has been issued, and comply with it; and • check the validity of the certificate (expiry, revocation, integrity) and of each certificate in the certification chain.

Type of information	Description
Users' obligation to verify the status of certificates	When a one-time-use certificate provided by the OTU CA is used, given the atomic nature of the signature operation computer-wise, the CP/CPS does not formulate any requirement regarding the obligation to verify the revocation of the Certificate. When an organization certificate provided by the OTU CA is used, the user must verify the status of the certificate that they intend to rely on before using it. For this, they can use the various tools that the OTU PKI puts at their disposal. In addition to the status, the user must check the validity of the certificate in question and that of the corresponding certification chain.
Limited guarantees and liability	The OTU CA undertakes to issue certificates in accordance with the CP-CPS and the state of the art. Through its services, the OTU PKI guarantees: • the authentication of the Subscriber by the Registration Authority through the Subscriber's Certificate; • the generation of one or more Certificates in accordance with the verified request of a Subscriber authenticated beforehand; • the provision, by the OTU CA, of functions that provide information about the statuses of the certificates issued, at the Subscriber's request, in accordance with this document; and • the exclusive control of the private key of the certificate by the Certificate Holder Mechanism, and the destruction of this key after a one-time-use session in the case of one-time-use certificates. No other guarantee is provided. The OTU PKI may only be held liable if the failure to comply with its obligations is proved. The OTU CA may in no case whatsoever be held liable in the event of a fault occurring within the scope of a Subscriber entity, and notably: • use of an expired Certificate, • use of a revoked Certificate, or • use of a certificate for a use other than those described in the section entitled "Restrictions of the use of certificates" of this document. Generally, the OTU CA is not responsible for the documents and information provided by the Subscriber and does not guarantee their accuracy or the detrimental consequences of facts, actions, negligence or omissions of the Subscriber, its representative or the Subject. The Subscriber is prohibited from making any commitment in the name and on behalf of the OTU CA, which it may not replace in any case whatsoever.
Applicable references	The applicable references are defined in section 1.3 of this document. The technical documentation of the OTU CA is available on its website at https://www.mediacert.com

Type of information	Description
Confidentiality policy	Worldline takes all the necessary measures to ensure the confidentiality of professional and personal data (see sections 9.3 and 9.4 of the CP-CPS) in accordance with the French legislation in force on the French territory.
Indemnification policy	The OTU CA delivers certificates as part of higher-level electronic services, notably electronic subscription services. The framework agreement signed between the Customer and Worldline or its duly authorized agent sets out the clauses with regard to indemnification should damage occur. If there is no such framework agreement, Worldline's General Terms of Sale will be applicable.
Applicable law	All of the OTU PKI's components including documentation are governed by the applicable legislation and regulations in force on the French territory even though some of the activities deriving from this CP/CPS might have legal effects outside of the French territory. The framework agreement signed between the Customer and Worldline or its duly authorized agent sets out the clauses with regard to dispute resolution. If there is no such framework agreement, Worldline's General Terms of Sale will be applicable. The authorized contact for any comment, request for additional information, claim or submission of a litigation file concerning the CP/CPS is defined in the "Point of Contact" section of this document.
CA audits	Worldline has the OTU PKI regularly audited by an independent, accredited body. These audits comply with standard [ETSI EN 319 411-1].