

PUBLIC

TIME-STAMPING SERVICE'S GENERAL
CONDITIONS OF USE

AUTHOR(S) : F. Da Silva
DOCUMENT NUMBER : WLS-TSA-F089
VERSION : 1.1
STATUS : Final
SOURCE : Worldline
DATE OF THE DOCUMENT : November 3, 2017
NUMBER OF PAGES : 9

DOCUMENT OWNER : Comité MediaCert

Table of contents

Table of contents	2
List of changes	3
1 Introduction	4
1.1 General presentation	4
1.2 Definitions of the terms.....	4
1.3 Acronyms	5
1.4 References	5
2 Details of the General Terms and Conditions of Use	6

List of changes

Version	Date	Description	Auteur(s)
0.1	03/11/2017	Initial version	F. Da Silva
1.0	30/03/2018	Validation of the document following the validation of the TP-TPS	F. Da Silva
1.1	05/07/2018	Addition of ETSI 319 421 OID	F. Da Silva

1 Introduction

1.1 General presentation

This document includes the essential provisions defined in the Time-stamping Policy - Time-stamping Practices Statements [TP-TPS] concerning the Time-stamping Service, in accordance with the regulations [EIDAS] and more particularly with the standard [ETSI 319 421]. These provisions include the commitments made by the Time-Stamping Authority, the procedures for using time-stamps and the respective obligations of the various parties concerned.

However, it is specified that because of its synthetic nature, this document does not replace the Time-stamping Policy - Time-stamping Practices Statements referred to in chapter 1.4.3 this document, available on the MediaCert *Trust Service Provider* website at the following address: <https://www.mediacert.com>.

This document also serves as the *TSA Disclosure Statement*.

The structure of this document is in accordance with Annex B2 "*TSA disclosure statement structure*" of the technical specification [ETSI 319 421].

1.2 Definitions of the terms

Subscriber: entity that needs to have data timestamped by a Time-Stamping Authority and that has accepted the conditions of use of its services.

Certification Authority: entity that produces and issues Certificates. This entity is in charge of the complete life cycle of these Certificates (creation, publication, revocation, etc.).

Time-stamping Authority: entity in charge of issuing and managing time-stamps in accordance with this TP-TPS.

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

Time-stamp: data that links a representation of a data to a particular time, expressed in UTC time, thus establishing proof that the data existed at that time.

Time-stamping: mechanism that consists in associating a date and time with an event, information or computer data in order to record the time at which an operation was performed.

Time-stamping Service: all the services required to generate and manage Time-stamps.

Time-stamping Unit: set of hardware and software in charge of creating Time-stamps characterized by an identifier of the Time-stamping Unit granted by a Certification Authority and by a unique Time-stamps signature key.

Universal Time Coordinated: time scale between international atomic time and universal time.

User: entity (person or system) that trusts a Time-stamp issued under the TP-TPS.

1.3 Acronyms

The acronyms used in this document are as follows:

- **CA:** Certification Authority;
- **TSA:** Time-Stamping Authority;
- **GCU:** General Terms and Conditions of Use;
- **TS:** Time-stamp;
- **TP-TPS:** Time-Stamping Policy - Time-Stamping Practices Statements;
- **TSS:** Time-Stamping Service;
- **TSP:** *Trust Service Provider*;
- **TSU:** Time-Stamping Unit.

1.4 References

1.4.1 Regulation

Reference	Description
[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

1.4.2 Technical regulations

Reference	Description
[ETSI 319 421]	ETSI EN 319 421 v1.1.1 (2016-03) Electronic Signature and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps OID: 0.4.0.2023.1.1
[ETSI 319 422]	ETSI EN 319 422 v1.1.1 (2016-03) Electronic Signature and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

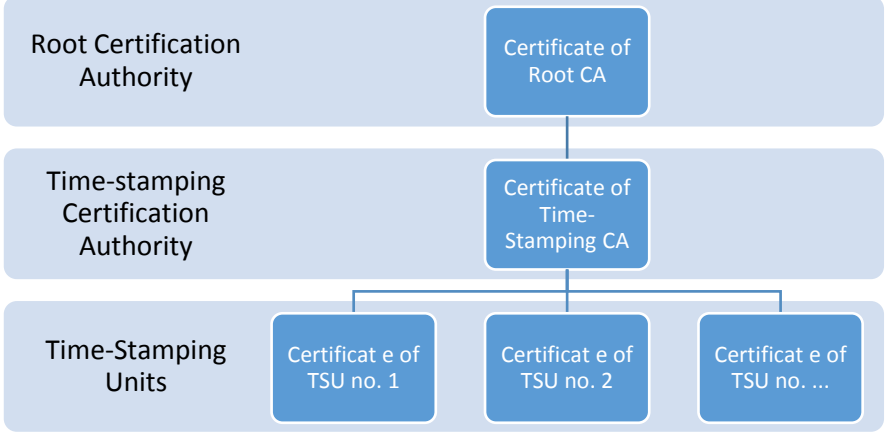
1.4.3 Worldline Documentation

Reference	Description
[GP]	General Policy of the TSP MediaCert TSP MediaCert Reference: WLM-TSP-F094 OID: 1.2.250.1.111.20.1.1
[TP-TPS]	Time-Stamping Policy - Time-Stamping Practices Statements Time-Stamping Authority Reference: WLM-TSA-F081 OID: 1.2.250.1.111.20.2.1

2 Details of the General Terms and Conditions of Use

Type of information	Description
Point of contact	<p style="text-align: center;">Comité MediaCert Worldline 23 rue de la Pointe Zone Industrielle A 59113 SECLIN France</p> <p style="text-align: center;">dl-mediacert-tsp@worldline.com</p>
How to obtain TSs	<p>The Subscriber sends his TS request to the TSS of Worldline's MediaCert TSP. This request must comply with the [ETSI 319 422] standard and must contain a fingerprint calculated by a state-of-the-art algorithm authorized by the [TP-TPS].</p> <p>The TS generated in response by the TSS then contains the fingerprint in question, a reliable time and is signed by the issuing TSU.</p> <p>To the extent possible, TSP MediaCert will implement appropriate approaches to make its TS issuance service accessible to any person with a disability, taking into account on a case-by-case basis the specificities of each applicant.</p>
Limitations of use of the service	<p>The Subscriber must use the service taking into account the limitations of the TSS, in particular:</p> <ul style="list-style-type: none"> • the service shall not be used for uses requiring accuracy greater than one (1) second, as indicated in the TS; • the limited validity period of the Certificates of the TSU; • the potential non-preservation of the TS by the TSA.
Service availability	<p>The targeted availability for the provision of the TS is 7 days a week, 24 hours a day, excluding preventive maintenance periods for the service.</p>

<p>Subscriber obligations</p>	<p>The TSS is open to any natural or legal person wishing to subscribe and benefit from the service, provided that it accepts these obligations.</p> <p>The Subscriber, if he/she wishes to benefit from the TSS:</p> <ul style="list-style-type: none"> • must accept and comply with these GCU; • is responsible for the correct calculation of the footprint of data and the link between the said time-stamped data and the TS produced; • undertakes to check the validity of the TSs as soon as they are received and to ensure that the fingerprint contained is identical to that submitted in the request; • is responsible for the conservation of TS to meet its own needs. <p>In addition, it is recommended that the Subscriber verify the status of the TSU Certificate issuing the TS at the time of the Time-stamp request.</p>
<p>Users obligations</p>	<p>The User must:</p> <ul style="list-style-type: none"> • verify that the TS has been correctly signed and that the TSU Certificate issuing the TS is valid at the time of the TS verification. The verification of a TS consists of: <ul style="list-style-type: none"> ○ verify the value of the fingerprint contained in the Time-stamp against the data to which it relates; ○ verify the signature present in the TS against the TSU Certificate that issued the TS; ○ verify the validity of the certification chain from TSU to the Root CA certificate. • take into account the limitations on the use of TS indicated in the section "<i>Limits on the use of the service</i>" of this document.

<p>TSU certificates</p>	<p>The TSs issued by a TSU are signed by its Certificate, dedicated to this use. This Certificate is issued by the MediaCert TSP Time-stamping CA, so the certification chain is as follows:</p>  <pre> graph TD Root[Root Certification Authority] --- RootCert[Certificate of Root CA] RootCert --- TSA[Time-stamping Certification Authority] TSA --- TSACert[Certificate of Time-Stamping CA] TSACert --- TSU1[Certificate of TSU no. 1] TSACert --- TSU2[Certificate of TSU no. 2] TSACert --- TSU3[Certificate of TSU no. ...] </pre> <p>Elements for verifying the validity of the TSU Certificates and the Time-Stamping CA Certificate (CRL, LAR) are available to Users on the MediaCert TSP's website at the following address: https://www.mediacert.com.</p>
<p>Limitations of warranty and liability</p>	<p>The TSA shall not be liable for any unauthorised or non-compliant use of the TSs. Indeed, the TSA can only be held liable in the event of proven non-compliance with its obligations.</p> <p>In addition, to the extent of the limitations of French law, the TSA cannot be held liable:</p> <ul style="list-style-type: none"> • no financial loss; • no data loss; • no indirect damage related to the use of a TS; • of any other damage. <p>In any event, the liability of the TSA shall be limited, for all events and for all damages combined, to the amount paid to the TSA for access to the Time-Stamping Service, in compliance with and within the limits of applicable law.</p>
<p>Trace retention time</p>	<p>In the context of these operations and in order to comply with legal and regulatory provisions, the TSA keeps records of the operations of its service for a period of ten (10) years, i.e. seven (7) years after the expiry of the TS.</p>
<p>Applicable references</p>	<p>The applicable references are defined in chapter 1.4 this document. The TSA public documentation is available on the MediaCert TSP's website at: https://www.mediacert.com.</p>

<p>Applicable law</p>	<p>The TSA, in all its components and including documentaries, is governed by the legislation and regulations in force on French territory applicable to it, although its activities arising from the [TP-TPS] may have legal effects outside French territory (see [GP]).</p>
<p>Force Majeure</p>	<p>Cases of force majeure will suspend the execution of the general conditions. Expressly, those usually retained by the case law of French courts and tribunals (see [GP]) are considered as cases of force majeure or fortuitous events.</p>
<p>Privacy Policy</p>	<p>Worldline takes all necessary measures to ensure the confidentiality of professional and personal data (see [GP]) in accordance with the applicable legislation defined in the section "<i>Applicable Law</i>" of this document.</p>
<p>Compensation policy</p>	<p>As part of the services provided, the Time-Stamping Authority does not provide any compensation.</p>
<p>Management of disputes and complaints</p>	<p>The authorized contact for any comments, requests for additional information, complaints or dispute files concerning the [TP-TPS] is defined in the "<i>Contact Point</i>" section of this document.</p> <p>In the event of a dispute relating to the interpretation, application and/or execution of this contract and failing to reach an amicable agreement, any dispute will be brought before the competent courts of Paris.</p>
<p>Applicable audits and references</p>	<p>As part of obtaining the qualification of the TSS within the meaning [eIDAS], Worldline regularly carries out an external certification audit of TSA to the [ETSI 319 421] standard by an independent and accredited body.</p>