PUBLIC

TIME-STAMPING POLICY - TIME-STAMPING PRACTICES STATEMENTS

AUTHOR(S)	:	F. Da Silva
DOCUMENT NO	:	WLM-TSA-F081
VERSION	:	1.1
STATUS	:	Final
SOURCE	:	Worldline
DATE OF THE DOCUMENT	:	October 26, 2017
NUMBER OF PAGES	:	25
DOCUMENT OWNER	:	Comité MediaCert

Role	Name	Signature	Date
Reviewer 1 – Head of TSP	Cyril Lootvoet	Cyril Lootvoet	05/07/2018
Reviewer 2 – ISSM	Nicolas Abrioux	Nicolas Abrioux	05/07/2018
Quality insurance function	Franck Da Silva	Franck Da Silva	05/07/2018
Document owner	Comité MediaCert	Cyril Lootvoet	05/07/2018

CYRIL LOOTVOET

Digitally signed by CYRIL LOOTVOET
DN: C=FR, L=SECLIN, O=Atos Worldline, OU=fr01.awl.atosorigin.net, SN=LOOTVOET, G=CYRIL, CN=CYRIL LOOTVOET, OID.0.9.2342.19200300.100.1.1=A536912, E=cyril.lootvoet@worldline.com
Reason: Validated by MediaCert Committee
Location:
Date: 2018-10-12 09:27:55

Table of contents

List of changes

Version	Date	Description	Author(s)
0.1	19/10/2017	Initial version	F. Da Silva
1.0	30/03/2018	Validation of the document by the Security Committee	Security Committee
1.1	05/07/2018	Addition of ETSI 319 421 OID Addition of the requirement related to the deadlines for publication of TSP MediaCert documentation Rescheduling of the steps to be carried out upon cessation of activity Removal of the TSA field in the TS profile	F. Da Silva

1 Introduction

1.1 General presentation

This document describes the "Time-Stamping Policy" of MediaCert *Trust Service Provider* established by Worldline to govern the Time-Stamping Service that can be used by its customers in two possible ways:

- either directly as a service in its own right;
- or indirectly through the electronic signature service offered by the same MediaCert *Trust Service Provider*.

This document presents in this context:

- the requirements with which the Mediacert *Trust Service Provider* complies as a Time-Stamping Authority;
- the generation and management of Time-stamps;
- obligations and requirements relating to the different actors.

In addition to describing the "Time-Stamping Policy", this document includes the public portion of the "Time-Stamping Practices Statements". This is a statement of the mechanisms and procedures used by the Time-Stamping Authority in the management of the Time-stamps it generates. The confidential elements of the Time-Stamping Practices Statements are recorded in a "Technical Documentation of Time-Stamping Practices" (TDTP).

This "Time-Stamping Policy – Time-Stamping Practices Statements" does not impose any requirement on the link between the digital fingerprint to be time-stamped and the content of the electronic data which requires that Time-stamp. This verification is the responsibility of the user.

The structure of this document is based on the documents from:

- [ETSI 319 421];
- [RGS A5].

The Time-Stamping Service, described by this document, being a trusted service of MediaCert, all [PG] requirements are, unless otherwise stated, applicable to the scope of this service.

The purpose of the Time-Stamping Service is to issue qualified Time-stamps within the meaning of the European Regulation [eIDAS]. To this end, the TSA is operated in accordance with the requirements of the following standards:

- [ETSI 319 421];
- [QUALIF TSA];
- [QUALIF TSP].

1.2 Document identification

Elements	Value
Title	Time-Stamping Policy - Time-Stamping Practices Statements
Document reference	WLM-TSA-F081
OID	1.2.250.1.111.20.2.1
Version	1.1
Author	F. Da Silva

The OID definition of the OID in this document is presented in [GP].

This document will be referred to as "TP-TPS" throughout the document.

1.3 Time-Stamping policy management

1.3.1 Entity managing the Time-Stamping Policy

This document does not add any information with respect to the [GP].

1.3.2 Entity determining the coherence of a Time-Stamping Practices Statements with this Time-Stamping Policy

This document does not add any information with respect to the [GP].

1.3.3 Approval procedure

This document does not add any information with respect to the [GP].

1.3.4 Point of contact

This document does not add any information with respect to the [GP].

1.4 Definitions and acronyms

1.4.1 Definitions of the terms

A list of the main definitions of the technical terms used in this TP-TPS is presented below.

Subscriber: entity that needs to have data time-stamped 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.

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

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. The whole is signed by the private key of the Certification Authority 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-stamp token: see Time-stamp.

Time-Stamping Service: all the services required to generate and manage time countermarks.

Time-Stamping System: all the Time-stamping Units and the administration and supervision components used to provide the Time-Stamping Service.

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-stamp signature key.

Universal Time Coordinated: is a time scale adopted as the basis of international civil time by the majority of countries around the world.

UTC(k) : reference time performed by the laboratory "k" (e.g.: Paris Observatory) and precisely synchronized with UTC time, with the aim of achieving an accuracy of ± 100 ns, according to recommendation S5 (1993) of the Advisory Committee for the Definition of the Second.

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

1.4.2 Acronyms

The acronyms used in this TP-TPS are as follows:

- **CA:** Certification Authority;
- **TSA:** Time-Stamping Authority;
- **GCU:** General Terms and Conditions of Use;
- **TS:** Time-stamp;
- **TDTP:** Technical Documentation of Time-Stamping Practices;
- **ETSI:** European Telecommunication Standards Institute;
- **CRL:** List of Revoked Certificates;
- **OID:** Object Identifier;
- **TP-TPS:** Time-Stamping Policy - Time-Stamping Practices Statements;
- **TSS:** Time-Stamping Service;
- **TSU:** Time-Stamping Unit;
- **UTC:** Universal Time Coordinated.

2 Responsibilities for the provision of information to be published

2.1 Entities responsible for making information available

This document does not add any information with respect to the [GP].

2.2 Information to be published

The information published by the Mediacert Committee on its website concerning the Time-Stamping Services are as follow:

- this TP-TPS written in French and English;
- the old versions of TP-TPS written in French and English;
- the current general conditions of use;
- the Certificate of each of the Time-Stamping Units governed by this document;

The [GP] provides information as to where the above information is made available.

2.3 Publication deadlines and frequencies

This document does not add any information with respect to the [GP].

2.4 Access controls to published information

This document does not add any information with respect to the [GP].

3 General provisions

3.1 Obligations of the Time-Stamping Authority

A number of obligations are imposed on the TSA. Indeed, the TSA must:

- provide a Time-Stamping Service (TSS) in accordance with the requirements and procedures prescribed in this TP-TPS. In particular, the TSA aims for a 7-day, 24/7 availability of its TSS;
- to fulfil all its commitments as stipulated in the GCU;
- ensure that the requirements and procedures defined in the TDTP are consistent with this TP-TPS;
- ensure compliance with the additional obligations imposed by the Certifying Authority that issued the Certificates of the Time-Stamping Units. In particular, the Certificates of the Time-Stamping Units are dedicated to the generation of TSs and are not used for any other purpose;
- inform stakeholders in the event that a TSU is compromised by its Time-Stamping System, as recalled in th e[GP].

3.2 Subscriber's Obligations

The Subscriber must accept and comply with the TSA's GCU if he/she wishes to benefit from the TSS.

The Subscriber is responsible for the correct calculation of the footprint of a data and the link between the time-stamped data and the TS produced.

The Subscriber 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.
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.

The Subscriber is responsible for the conservation of the TSs to meet his/her own needs.

The Subscriber must use the service taking into account the limitations of the TSS, in particular:

- the service must not be used for uses requiring greater accuracy than that indicated in the TS;
- the limited validity period of the Certificates of the Time-Stamping Units;
- the potential non-compliance of the TS by the TSA.

All these obligations are included in the [GCU] of the service.

3.3 Obligations of the User

The User must:

- 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;
- take into account the limitations on the use of the TS indicated in this document and in the [GCU], in particular taking into account the validity period of the Time-Stamping Unit Certificate.

The validation of a Time Countermark consists of:

- compare the hash contained in the TS to the hash of the Time-stamped document;
- validate the certification chain from the TSU Certificate to the trusted root;
- ensure that no Chain of Trust Certificate has been revoked prior to the establishment of the TS. This can be easily achieved using the CRLs published by the CAs issuing the said Certificates (see [CP-CPS]).

Beyond the period of validity of the TSU Certificate, the following additional elements must be verified:

- ensure that the TSU private key has not been compromised;
- that the hash algorithm still has the necessary robustness and that the existence of collisions has not been detected;
- that the signature algorithm and key size used in the TS signature is still cryptographically robust at the time of verification.

Alternatively, secure storage or renewal of the TS are methods that can be implemented and demonstrate the validity of the TS beyond the validity period of the TSU Certificate.

3.4 Time-Stamping Practices Statements

The TSA ensures that it has the necessary reliability to provide the TS and describes its implementation within this document. In particular:

- the TSA regularly carries out a risk analysis to identify ISS risks and the ISS measures then implemented to address these risks;
- the TSA has a TDTP used to address all the technical requirements identified in this TP-TPS;
- the TSA makes available to Subscribers and Users the public elements of its TDTP within this document so that they can assess its conformity;
- the TSA has an appropriate organisation for the approval of this TP-TPS and the verification of the concordance between the TDTP and the TP-TPS (see chapter 1.3.3);
- the person in charge of the TSA ensures that the practices are properly implemented;
- the TSA regularly conducts audits to ensure compliance of practices, including responsibilities, with the TDTP (see chapter 8);
- if the TSA has been certified in accordance with this TP-TPS and if a proposed change to its initiative may result in non-compliance with this TP-TPS or with the TDTP, then the TSA shall submit such change to the independent certification body for advice.

3.5 General Terms and Conditions of Use

The TSS's [GCU] reflect the main principles described in this document. They are based on the model defined in Annex B of [ETSI 319 421].

These [GCU] are made available to Subscribers and Users on the publication site (see chapter 2.2).

3.6 Compliance with legal requirements

3.6.1 Confidentiality of professional data

This document does not add any information with respect to the [GP].

3.6.2 Personal data

Within the framework of the services provided by the Time-Stamping Authority governed by this TP-TPS, there is no handling of personal data requiring a CNIL declaration. All requirements from the [GP] concerning personal data are therefore not applicable to the TSS perimeter.

3.6.3 Provisions concerning conflict resolution

The authorized contact for any comments, requests for additional information, complaints or submission of dispute files concerning this TP-TPS is defined in chapter 1.3.4.

In the event of a dispute relating to the interpretation, application and/or execution of this document and failure to reach an amicable agreement, any dispute will be brought before the competent courts in Paris.

3.6.4 Indemnities

Not applicable.

4 Operational requirements

4.1 Management of Time-stamp requests

The Subscriber sends his TS request to the TSS of Worldline's MediaCert TSP. This request must comply with the [RFC 3161] standard, taking into account the restrictions of the [ETSI 319 422] standard, and must contain a fingerprint calculated by a state-of-the-art algorithm authorized by the TP-TPS (see chapter 6.7).

The TSA provides a TS in response to a request containing the fingerprint of the data to be time-stamped. The provision of the TS does not exceed a few seconds [1], in order not to harm or degrade the ergonomics of the calling application.

The TS generated in response by the TSS then contains the fingerprint in question, a reliable time and is signed by the issuing TSU.

4.2 Audit files

4.2.1 Type of data constituting the audit files

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

The TSA shall retain relevant information concerning the data issued and received, in particular for the purpose of providing evidence in court. Among this information are the related elements:

- to the administration of the TSS;
- the operation of the TSS;
- the life cycle of the TSU Key pairs;
- the life cycle of TSU Certificates ;
- events related to clock synchronization of TSUs, including events related to the detection of loss of synchronization and recalibration of the TSU clock.

The TSA governed by this TP-TPS reserves the right to retain the TSs generated by its TSUs.

4.2.2 Retention period for audit files

Unless otherwise specified, audit files are kept for a period of ten (10) years, seven (7) years after the expiry of the TS.

4.2.3 Protection of audit files

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

[1] This response time is the time between the receipt of the request and the signature of the resulting TS.

4.3 Private key life management

The TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. For this purpose, operational and technical procedures are put in place and defined within the TDTP.

The lifetime of TSU private keys is defined in chapter 6.10 this document.

4.4 Clock synchronization

The TSA guarantees that its clock is synchronized with UTC time according to the declared accuracy of one (1) second.

More specifically:

- The synchronization with UTC is guaranteed by synchronizing the TSU clock with the servers of a recognized UTC(k) laboratory (see chapter 6.1);
- the calibration of each TSU clock is maintained in such a way that the clocks cannot normally drift outside the declared accuracy;
- TSU clocks are protected against threats to their environment that could lead to desynchronization with UTC time outside the declared accuracy;
- the TSA guarantees that any failure to comply with the accuracy announced by the internal clock of one of its TSUs will be detected;
- if the clock of a TSU is detected as being outside the declared accuracy, or the time servers are no longer available, then the TSs will no longer be generated until the clock of the TSU is resynchronized;
- TSA ensures that clock synchronization is maintained when a second jump is programmed as notified by the appropriate body. The change to take into account the second jump is made during the last minute of the day on which the second jump is scheduled.

4.5 Requirements of the content of a Time-stamp

The TSs issued by the TSUs of the TSA governed by this TP-TPS are generated in Worldline's secure premises and include a time established in accordance with the requirements of section 4.4. These TSs comply with the standard [ETSI 319 422] and therefore with the standard [RFC 3161].

Each TS is signed by the private key, reserved for this purpose, of the issuing TSU (see chapter 6.3).

These TS are made up as described in chapter 7.2 this document.

4.6 Compromise of the Time-Stamping Authority

In the case of events that affect the security of the TSS or the TSs issued or in the case of events that are likely to do so, the TSA ensures that appropriate information is made available to Subscribers and Users.

These events include, in particular:

- the compromise, real or suspected, of the private key of a TSU having a Certificate issued by the TSA governed by this TP-TPS;
- the prolonged loss of connection with time servers;
- the detected loss of calibration of the clock of a TSU having a Certificate issued by the TSA governed by this TP-TPS.

The [GP] defines the procedures and policies to be applied in the event of an incident.

In the event of compromise, suspected compromise, or erroneous TS issuance following a loss of calibration, the TSA will notify the Subscribers and Users affected, as well as the ANSSI. The TSU causing the compromise will be deactivated until the actual correction or lifting of the suspicion is corrected.

4.7 End of activities

As defined in the [GP], a business termination plan is defined and maintained for the TSA. It will be applied when Worldline has to discontinue the TSS governed by this document. This plan enables the TSA to ensure that potential disruptions to Subscribers and TS Users are minimised following the cessation of TSS activity and in particular ensures the continuous maintenance of the information necessary to verify the accuracy of TS.

This plan includes the following points, among others:

- before terminating its TSS, the following procedures will be performed:
  - the TSA will make available to all its Subscribers and Users information concerning its end of activity;
  - the TSA shall notify the contact point of the national supervisory body (ANSSI) directly and without delay of the cessation of activity;
- when stopping its TSS, the following procedures will be performed:
  - the TSA formalises the end of the contract with the Subscribers;
  - the TSA will request the revocation of all its Certificates;
  - the TSU private keys will be destroyed in such a way that they cannot be recovered (see chapter 6.6);
  - the TSA will revoke the authorisations given to potential subcontractors to act on its behalf in the performance of any functions relating to the TS generation process;
  - the TSA will transfer to Worldline its obligations to maintain the audit files and records necessary to demonstrate its correct functioning for a period of at least ten (10) years from the effective end of its activity;
  - the TSA will transfer to a Worldline its obligations to make its public keys and Certificates available to Users for a minimum period of ten (10) years from the effective end of activity.

- the TSA shall take the necessary measures to cover the expenses to fulfil the above requirements in the event that the TSA becomes bankrupt or for other reasons is unable to cover the expenses by itself.

4.8 Revocation of a Time-Stamping Unit Certificate

4.8.1 Reason for revocation

The TSA may request the revocation of a TSU Certificate for the following reasons, among others:

- early end of life of the TSA or TSU;
- compromise or suspicion of compromise of the TSU private key.

All the reasons for a request to revoke a TSU Certificate are described in the [CP-CPS] of the Time-stamping CA issuing the relevant Certificate.

4.8.2 Revocation procedure

The procedure for revoking a Time-Stamping Unit Certificate of the MediaCert TSP is internal and is specified in the TDTP. This complies with the requirements described in [CP-CPS] of the Time-Stamping CA issuing the relevant Certificate.

5 Physical and environmental, procedural and organisational requirements

5.1 Physical and environmental requirements

5.1.1 Geographical location and site construction

This document does not add any information with respect to the [GP].

5.1.2 Physical access

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

In particular, the critical systems of the Time-Stamping Service, in particular the TSUs, are operated in a secure area (see [GP]) used by all MediaCert TSP's Trust Services.

Indeed, access control measures are put in place to physically protect the HSMs of the TSA from unauthorised access, in particular:

- within the secure environment where they are stored;
- during their possible temporary storage before production.

This secure environment physically and logically protects TSS systems and data against unauthorized access that could lead to compromise.
In particular, the following measures are in place:

- each entry and exit from the secure area is traceable;
- the entry and exit of the zone are subject to independent supervision;
- any person with non-permanent access is monitored by a person in a trusted role in all secure areas.

Only personnel in a trusted role are authorized to access secure areas.

5.1.3 Power supply and air conditioning

This document does not add any information with respect to the [GP].

5.1.4 Vulnerability to water damage

This document does not add any information with respect to the [GP].

5.1.5 Fire prevention and protection

This document does not add any information with respect to the [GP].

5.1.6 Conservation of the supports

This document does not add any information with respect to the [GP].

5.1.7 Decommissioning of supports

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

In particular, in the event of deactivation of an HSM, the TSU keys are deleted beforehand using the "zeroization" functions of the HSM.

Equipment, data, media and software operated in the secure area may not be removed from the site without authorization.

5.1.8 Off-site backups

This document does not add any information with respect to the [GP].

5.2 Procedural requirements

5.2.1 Trusted roles

This document does not add any information with respect to the [GP].

5.2.2 Number of people required per task

This document does not add any information with respect to the [GP].

5.2.3 Identification and authentication for each role

This document does not add any information with respect to the [GP].

5.2.4 Roles requiring segregation of duties

This document does not add any information with respect to the [GP].

5.2.5 Operational management

The TSA ensures that the components of the Time Stamping System are safe and properly operated, with a minimal risk of failure. In addition, the TSA is setting up a quality and security management system for the information system within the scope of the timestamping service.

5.2.5.1 Data and software exchange

This document does not add any information with respect to the [GP].

5.2.5.2 Technical security measures specific to computer systems

This document does not add any information with respect to the [GP].

5.2.5.3 Network security measures

This document does not add any information with respect to the [GP].

5.2.5.4 Handling and security of the supports

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

In particular, with regard to the management and conservation of media, the TSA ensures the monitoring and security of HSMs protecting the keys of TSU throughout their life cycle in particular, the TSA, through organisational security measures, ensures that the HSMs could not be altered:

- during their transport;
- during their temporary storage before installation on the secure production site.

5.2.5.5 System planning

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

In particular, the TSA monitors its ability to process the volume of requests and makes projections to ensure an adequate scale-up of the service.

5.2.5.6 System qualification

The Time-Stamping Unit linking the date and time to the time-stamped data is composed of:

- a Time-stamping application;
- an HSM in accordance with Chapter 6.2.

The TSA certifies its TSS to ensure an adequate level of safety.

5.2.5.7 Incident reporting and response

This document does not add any information with respect to the [GP].

5.2.6 Access management to the Time-Stamping System

All requirements of the [GP] apply. In particular, the TSA shall configure the systems operating the TSUs so that all accounts, applications, services, protocols and ports not required for the Time-Stamp Services are deleted or disabled.

5.2.7 Deployment and maintenance

This document does not add any information with respect to the [GP].

5.3 Organizational requirements

5.3.1 Required qualifications, skills and authorizations

All requirements of the [GP] are applicable. In particular, the TSA employs a sufficient number of staff to operate its trusted Time-Stamping Service. The staff shall have the technical skills, experience and training necessary to carry out the tasks necessary for the operation of the TSA.

5.3.2 Background check procedures

This document does not add any information with respect to the [GP].

5.3.3 Initial training requirements

This document does not add any information with respect to the [GP].

5.3.4 Continuing education requirements and frequencies

This document does not add any information with respect to the [GP].

5.3.5 Frequency and sequence of rotation between different allocations

This document does not add any information with respect to the [GP].

5.3.6 Sanctions in the event of unauthorized actions

This document does not add any information with respect to the [GP].

5.3.7 Requirements for the staff of external service providers

This document does not add any information with respect to the [GP].

5.3.8 Documentation provided to staff

This document does not add any information with respect to the [GP].

6 Technical safety requirements

6.1 Time accuracy

TSA guarantees that the TSs generated by its TSUs have a maximum time difference of one (1) second compared to the time provided by the UTC(k) laboratory[2]. This accuracy is obtained by synchronizing and controlling the clocks of the TSUs based on two different time sources, including at least one UTC(k) reference.

6.2 Key generation

The conditions for generating TSU Key pairs are defined in the [GP]. In particular, the TSU keys are generated on MediaCert TSP's premises by at least two (2) authorized persons in a trusted role. As indicated in the general policy, TSU keys are generated in an HSM. This HSM is the subject of:

- compliance with common criteria at an EAL4 level or higher;
- a qualification at the level reinforced by ANSSI.

Each TSU has only one active private key at a time. The renewal of the Certificate without renewal of the Key pair is not authorized by this TP-TPS. TSU keys are only used in HSMs that have been used for their generation (see chapter 6.5).

6.3 Certification of the keys of the Time-Stamping Unit

The TSU Certificates governed by this TP-TPS are generated by the Time-Stamping CA in accordance with the requirements defined in the associated [CP-CPS]. The TSA also complies with its obligations, as defined in the corresponding [CP-CPS].

When a TSU Certificate is issued by the Time-Stamping CA, the TSA checks the entire chain of the Certificate and in particular:

- that the Certificate is issued by the required CA;
- that it conforms to the expected template.

The TSA ensures that the TSU can only be operational once these checks have been successfully completed. Under no circumstances will a TSU be able to generate TSs before the verification, installation and publication of its certificate.

6.4 Protection of the keys of the Time-Stamping Units

This document does not add any information with respect to the [GP].

6.5 Backup requirements for keys of Time-Stamping Units

[2] For deviations of the order of the second (usually a few tens of nanoseconds at the most), the difference between UTC and the UTC(k) source used is considered negligible.

The backup of TSU keys is prohibited by this TP-TPS.

6.6 Destruction of the keys of the Time-Stamping Units

Since the private key of the TSU is not backed up (see chapter 6.5), the destruction of the instance of the key present in the HSM, via the functionalities of the latter, allows its permanent destruction.

6.7 Mandatory algorithms

The TSA accepts algorithms for the calculation of digital fingerprints by Subscribers that are compatible with the best practices and recommendations of ANSSI and the standard [ETSI 119 312]. Here is the list:

- SHA-256 ;
- SHA-512.

The size of the Key pairs and the algorithms used by the TSUs used to sign the TSs comply with the requirement s[ETSI 119 312]:

Algorithm	Hash function	Size (bits)
RSA	SHA-256	2048

MediaCert TSP is authorized to develop these algorithms according to the state of the art of cryptanalysis and ANSSI's recommendations.

6.8 Checking Time-stamps

The TSA ensures that Users have access to the information necessary to verify the digital signature of TS. TSU Certificates are attached to the TSs and available on the *Trust Service Provider* MediaCert institutional website (in accordance with the [CP-CPS]).

6.9 Period of validity of the public key Certificates of the Time-Stamping Units

TSU public key Certificates have a lifetime of three (3) years. The TSA ensures that the lifetime of these Certificates complies with the algorithm and associated key size used in accordance with [ETSI 119 312] and ANSSI recommendations.

6.10 Useful life of the private keys of the Time-Stamping Units

The useful life of TSU private keys is less than the life of the associated Certificate (see chapter 6.9).
The period of use of TSU private keys is limited in practice to one (1) year in order to facilitate the verification of Time-stamp tokens through an appropriate period of validity of the Certificate (see chapter 6.9).
The TSS automatically rejects any TS request if the validity limit of the private key is exceeded.

7 Profile of Certificates and Time-stamps

7.1 Certificate of Time-Stamping Unit

Information about the profile of TSU Certificates is available in the [CP-CPS].
These Certificates are issued by a dedicated CA operated by MediaCert TSP in accordance with the [ETSI 319 411-2] standard at the QCP level.

7.2 Time-stamps

Field	Description	Value
version	Format version	1
policy	OID of the TP-TPS applied	1.2.250.1.111.20.2.1
messageImprint	OID of the hash algorithm of the data to be time-stamped	Same as the values included in the request
serialNumber	Unique identifier of the TS. This identifier can be a maximum of 160 bits.	Generated by the TSU
genTime	Time at the time of TS generation, synchronized with UTC time	TSU time at time of generation
accuracy	Declared accuracy of the TS in accordance with the TP-TPS applied	1 second
ordering	Scheduling information	False
nonce	Anti-replay data	Same as in the application (if present)

8 Compliance audit and other evaluations

8.1 Frequency and/or circumstances of evaluations

Worldline, as part of the TSS's qualification, conducts an external certification audit of the TSA to the [ETSI 319 421] standard every two (2) years by an accredited organization.

In addition, Worldline carries out a surveillance audit (internal or external) between two (2) external audits of Certification to the standard [ETSI 319 421].

8.2 Identities / qualifications of assessors

8.2.1 Certification audit

This document does not add any information with respect to the [GP].

8.2.2 Surveillance audit

This document does not add any information with respect to the [GP].

8.3 Relations between evaluators and evaluated entities

8.3.1 Certification audit

This document does not add any information with respect to the [GP].

8.3.2 Surveillance audit

This document does not add any information with respect to the [GP].

8.4 Topics covered by the evaluations

This document does not add any information with respect to the [GP].

8.5 Actions taken in response to evaluation findings

This document does not add any information with respect to the [GP].

8.6 Communication of results

This document does not add any information with respect to the [GP].

9 Appendices

9.1 Regulations and regulations

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
[GDPR]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

9.2 Documentary references

9.2.1 Technical regulations

Reference	Description
[ETSI 119 312]	ETSI EN 119 312 v1.2.1 (2017-05) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI 319 401]	ETSI EN 319 401 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[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
[RFC 3161]	Network Working Group - August 2001 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[RGS A5]	Time-stamping Policy Type v3.0 General Safety Framework (GSR) version 2.0 - Appendix A5 Reference: RGS_v-2-0_A5
[QUALIF TSA]	Qualified electronic timestamping services - Criteria for assessing compliance with the eIDAS Regulation Agence nationale de la sécurité des systèmes d'information (ANSSI) Version 1.1 of January 3, 2017
[QUALIF TSP]	Qualified trusted service providers - Criteria for assessing compliance with the eIDAS Regulation Agence nationale de la sécurité des systèmes d'information (ANSSI) Version 1.2 of July 05, 2017

[ETSI 319 411-2]	ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

9.2.2 Worldline Documentation

Reference	Description
[GCU]	General Terms and Conditions of Use Time-Stamping Authority Reference: WLM-TSA-F089
[CP-CPS]	Certification Policy - Certification Practices Statements TSP MediaCert Reference: WLM-TSP-F104 OID: 1.2.250.1.111.20.3.1.2
[GP]	General Policy of the MediaCert TSP TSP MediaCert Reference: WLM-TSP-F094 OID: 1.2.250.1.111.20.1.1