MEDIACERT TSP'S GENERAL POLICY

AUTHOR(S)	:	F. Lesecq
DOCUMENT NO	:	WLM-TSP-F094
VERSION	:	1.5
STATUS	:	Final
SOURCE	:	Worldline
DATE OF THE DOCUMENT	:	January 27, 2020
NUMBER OF PAGES	:	48

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: 2020-03-03 12:03:07

Role	Name	Signature	Date
Reviewer 1 – Deputy Head of TSP	Fanny Lesecq	Fanny Lesecq	27/01/2020
Reviewer 2 - ISSM	Didier Sobkowiak	Didier Sobkowiak	27/01/2020
Quality insurance function	Fanny Lesecq	Fanny Lesecq	27/01/2020
Document owner	MediaCert Committee	Guillaume Bailleul	27/01/2020
Approver – Head of TSP	Guillaume Bailleul	Guillaume Bailleul	27/01/2020

Table of contents

Table of contents 2
List of changes 5
1 Preface 6
1.1 References 6
1.2 Definitions of the terms 7
1.3 Acronyms 7
2 Introduction 9
2.1 Object 9
2.2 Document identification 9
2.3 Structure of the General Policy 9
3 Scope of the General Policy 10
3.1 Functional scope 10
3.2 Technical scope 10
4 Security risk analysis 11
5 Policies and Practices 12
5.1 Management of MediaCert TSP's documentation 12
5.2 Provision of information 13
5.3 Amendments to the GP, CP-CPS, TP-TPS and AP 15
5.4 Technical Documentation of General Practices 16
5.5 Applicable information security policies 16
6 Organization of the management of Trust Services 17
6.1 Functions and responsibilities related to Trust Services 17
6.2 Number of people required 18
6.3 Identification and authentication for each role 18
6.4 Separation of roles 18
6.5 Relations with the authorities 18
6.6 Relations with suppliers 19
6.7 Governance bodies 19
6.8 Independence of the parties and non-discrimination 19
7 Human Resources Security 21
7.1 Required qualifications, skills and authorizations 21
7.2 Background check procedures 21
7.3 Initial training requirements 22
7.4 Continuing education requirements and frequencies 23
7.5 Frequency and sequence of rotation between different allocations 23
7.6 Sanctions in the event of unauthorized actions 23
7.7 Requirements for the staff of external service providers 23
7.8 Documentation provided to staff 23
8 Asset Management 24
8.1 Asset Responsibilities 24

8.2 Classification of information 24
9 Access control 25
9.1 Physical access 25
9.2 Logical access 25
9.3 Network access 25
9.4 Management of access rights 25
9.5 Manage accounts, passwords and sessions 25
10 Cryptographic measurements 27
10.1 Standards and security measures for cryptographic modules 27
10.2 Key pair management 27
10.3 CA private key activation data 29
11 Physical and environmental security 30
11.1 Geographical location and site construction 30
11.2 Power supply and air conditioning 30
11.3 Vulnerability to water damage 30
11.4 Fire prevention and protection 30
11.5 Decommissioning of supports 30
12 Operational management 32
12.1 Computer system security measures 32
12.2 Operating procedures and responsibilities 33
12.3 Protection against malware 33
12.4 Backups 33
12.5 Logging and monitoring 33
12.6 Mastery of software in operation 34
12.7 Technical vulnerability management 34
12.8 Acquisition, development and maintenance of information systems 35
13 Communications Security 36
13.1 Network access management 36
13.2 Information transfer 37
13.3 Redundancy 37
14 Incident management 38
14.1 Security incident management 38
14.2 Security incident management procedures 38
15 Collection of evidence 39
15.1 Logging 39
15.2 Archiving 40
16 Business continuity 42
16.1 Availability commitments 42
16.2 Business continuity and recovery 42
17 End of activities 43
18 Conformity 44
18.1 Insurance 44

18.2 Confidentiality of professional data 44
18.3 Protection of personal data 45
18.4 Intellectual and industrial property rights 46
18.5 Provisions concerning conflict resolution 46
18.6 Competent jurisdictions 46
18.7 Compliance with laws and regulations 47
18.8 Force majeure 47
18.9 Audits 47

List of changes

Version	Date	Description	Author(s)
0.1	14/11/2017	Initialization of the document	F. Da Silva N. Shelters V. Dumond
1.0	30/03/2017	Validation of the document by the Security Committee	Security Committee
1.1	05/07/2018	Integration of post-audit remarks internal to the timestamping platform: Modification of the deadline for publication of MediaCert TSP documentation Modification of the presentation scheme of the MediaCert TSP	F. Da Silva C. Lootvoet
1.2	18/09/2018	Integration of the Electronic Archiving Service into the scope of the MediaCert TSP Consideration of the integration of a new CA (the LCP OTU CA) which only leads to a change in the functional scope of the GP	F. Da Silva
1.3	12/10/2018	Consideration of the remarks/deviations detected during the 2018 certification audit of the AC OTU LCP: • separation of tasks for review/validation and approval of documents	F. Da Silva
1.4	23/04/2019	Clarification of the contact point of the TSP MediaCert: it concerns not only documentation but also all forms of requests. Consideration of possible foreign service providers in the verification of criminal records because bulletin n°3 is specifically French. Evolution of the versions of the standards of the repository.	F. Da Silva
1.5	27/01/2020	Adding new MediaCert CA 2019's	F. Lesecq

1 Preface

1.1 References

1.1.1 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
[SIAF]	Heritage Code Decree n°2011-574 of 24 May 2011 Book 2
[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

1.1.2 Technical regulatory references

Reference	Description
[ETSI 119 312]	ETSI EN 119 312 v1.2.2 (2018-09) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI 319 401]	ETSI EN 319 401 v2.2.1 (2018-04) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ISO 27001]	ISO/IEC 27001 : 2013 Information technology - Security techniques - Information security management systems - Requirements
[ISO 27002]	ISO/IEC 27002 : 2013 Code of good practice for safety management of information
[Hygiene]	Computer hygiene guide - Reinforce the security of your information system sound in 42 steps National Agency for Information Systems Security (ANSSI)
[ANSSI Qualification]	Qualified trusted service providers Criteria for assessing compliance with the eIDAS v1.1 Regulation National Agency for Information Systems Security (ANSSI)
[RGS B1]	General Safety Standard v2.0 - Appendix B1 (2014-02) National Agency for Information Systems Security (ANSSI) Cryptographic mechanisms: rules and recommendations for the selection and sizing of cryptographic mechanisms
[SOGIS_CRYPTO]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version in force. Available at http://sogis.org

1.2 Definitions of the terms

A list of the main definitions of the technical terms used in this GP is provided below:

Subscriber: an entity/organization that benefits from one or more trusted services provided by MediaCert TSP.

Bi-key: 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 fingerprint *(digest*) or the criteria for use. The whole is signed by the private key of the Certification Authority that issued the Certificate.

Archiving Service: a service that includes a set of actions aimed at identifying, collecting, classifying, storing, storing, communicating and returning electronic documents, for the time necessary to satisfy legal obligations or for information needs or for property purposes.

Certification Service: service that produces Certificates and, more generally, manages them (manufacturing, delivery, revocation, publication, logging, archiving) in accordance with a certification policy.

Trust Service: a trust service is an electronic service that consists of:

- the issuance of electronic signature, electronic stamp and website authentication certificates; or
- the validation of electronic signatures and stamps; or
- the storage of electronic signatures and electronic stamps;
- electronic time stamping;
- electronic registered mail.

Electronic archiving of information (other than the storage of electronic signatures and electronic stamps) is not considered a trusted service within the meaning of the Regulation [eIDAS]. However, as it is operated under conditions similar to the certificate issuance and timestamping services provided by MediaCert TSP, electronic archiving will be considered as a trusted service within MediaCert TSP and therefore within this document.

Time-stamping service: service that produces time stamps and more generally ensures their management in accordance with a time-stamping policy.

1.3 Acronyms

A list of acronyms used in this GP is provided below:

- **CA:** Certification Authority;
- **AFNOR:** French Standards Association;
- **TSA**: Time-Stamping Authority;
- **TDGP:** Technical Documentation of General Practices;
- **EIDAS:** Electronic IDentification And Signature;
- **HSM :** Hardware Security Module;

- **PKI:** Public Key Infrastructure;
- **CR**: List of Revoked Certificates;
- **OID:** Object IDentifier;
- **CP-CPS:** Certification Policy - Declaration of Certification Practices;
- **TP-TPS:** Time-Stamping Policy - Time-Stamping Practices Statements;
- **AP:** Archiving Policy;
- **PCRA**: Continuity and Business Resumption Plan;
- **GP:** General Policy of the MediaCert TSP;
- **IMP:** Incident Management Policy;
- **ISP:** Worldline Information Security Policy;
- **GDPR:** General Data Protection Regulations;
- **EAS:** Electronic Archiving Service;
- **SIAF:** Service Interministériel des Archives de France;
- **SIEM:** Security Information & Event Management;
- **SOC:** Security Operation Center ;
- **ISS**: Information Systems Security;
- **TSP**: Trust Service Provider;
- **TSU**: Time Stamping Unit.

2 Introduction

2.1 Object

The MediaCert *Trust Service Provider,* established by Worldline, provides a set of Trust Services and is therefore subject to a set of regulations (see chapter 1.1.1) such as the "eIDAS" Regulation No 910/2017 of the European Parliament and of the European Council on electronic identification and trust services for electronic transactions in the internal market.

This document describes the general policy of MediaCert TSP. In this context, it presents:

- the general requirements to which the MediaCert TSP is subject;
- the organization set up to ensure the provision of services;
- the general security measures applied.

2.2 Document identification

Elements	Value
Title	MediaCert TSP's General Policy
Document reference	WLM-TSP-F094
OID	1.2.250.1.111.20.1.1
Version	1.5
Author	F. Lesecq

The OID definition of this document is presented in chapter 5.3.2.1.

This document will be referred to as "GP" throughout the document.

2.3 Structure of the General Policy

In order to facilitate interoperability with applicable standards, this GP is structured in accordance with:

- the clauses of the standard [ETSI 319 401];
- the main clauses of the standard [ISO 27002].

3 Scope of the General Policy

3.1 Functional scope

As defined in the introduction, this document describes the general policy adopted and applied by all MediaCert TSP's Trust Services, regardless of their level of qualification, in accordance with the eIDAS regulation.

Among the Trust Services provided are the following:

- the issuance of electronic signature and electronic stamp certificates;
- electronic time stamping;
- electronic archiving (see chapter 1.2).

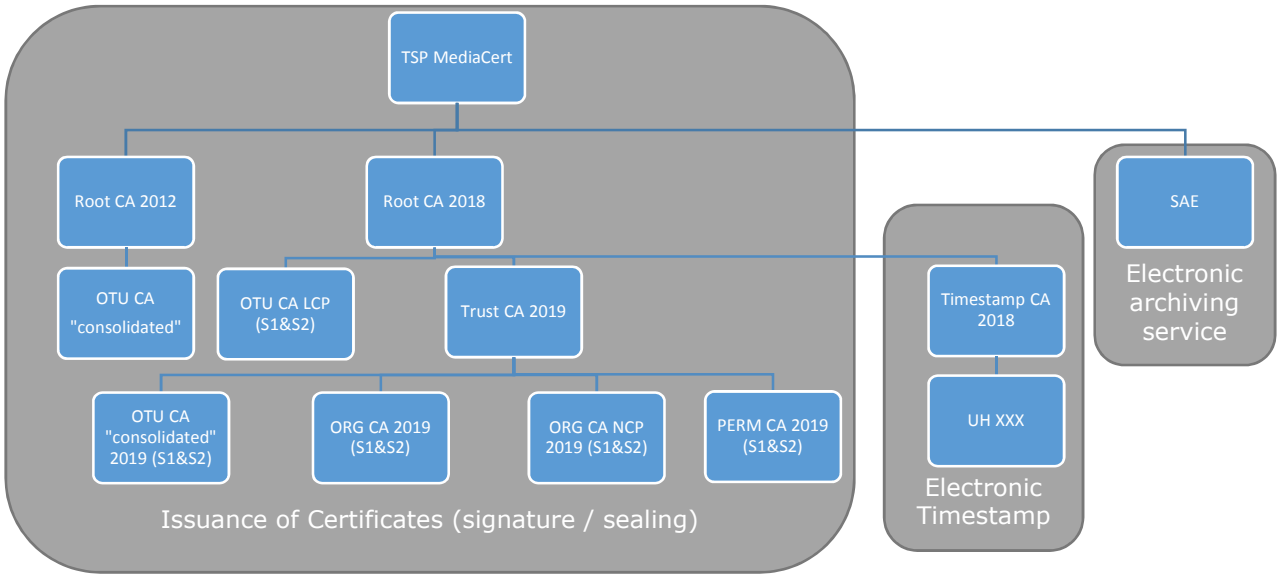

Figure 1 - Functional scope of the MediaCert TSP

3.2 Technical scope

This GP applies to the entire scope of MediaCert TSP. These components are presented in the TDGP as well as in the technical documentation specific to each MediaCert TSP's Trust Service.

4 Security risk analysis

As part of MediaCert TSP's activities, a risk analysis is carried out by the MediaCert TSP's security manager within the scope of the Trust Services.

Its objective is to enable the identification, analysis and assessment of ISS functional and business risks, and to enable the definition of appropriate measures implemented to deal with them, taking into account the results of the assessment.
Risk management measures ensure that the level of security implemented is proportionate to the risks weighing on the IS.
It ensures that the TDGP (see chapter 5.4) is consistent with the level of risk by determining all necessary safety requirements and operational procedures.

This document makes it possible to identify the depreciation of algorithms, assets and their security needs applicable to MediaCert TSP's systems. It takes into account the state of the art in this field and is subject to regular revision, at least once a year, and in the event of major changes in infrastructure or services. It is validated by the MediaCert Committee, which accepts the residual risks exposed, following its regular review (see chapter 6.7).

In the case of a qualified service, the MediaCert TSP will proceed to the approval of the service according to the recommendations of the ANSSI [ANSSI Qualification] before providing the Qualified Trust Service. This approval is reviewed every two (2) years.

Risk analysis also makes it possible to identify sensitive data. As such, they are subject to specific security measures that may include backup, logging, access, etc.

5 Policies and Practices

5.1 Management of MediaCert TSP's documentation

5.1.1 Entity managing the documentation of the MediaCert TSP

Worldline is responsible for the development, approval, monitoring and revision, as necessary, of the MediaCert TSP's documentation. To this end, a committee called the "MediaCert Committee" is set up as defined in chapter 6.7 of this document.
In particular, for each Trusted Service operated by MediaCert, a Trusted Service Policy, as well as practices supporting this policy, are developed and documented.
This document defines and documents the requirements and practices common to all MediaCert trust services, specific additional requirements and practices are detailed in the documentation specific to each of the Trust Services.

Among the relevant MediaCert TSP's documentation are the following:

- this General Policy;
- Certification Policy - Certification Practices Statements;
- Time-Stamping Policy - Time-Stamping Practices Statements;
- Archiving Policy;
- Risk analysis.

All these documents, as well as this document, are subject to approval by the Head of the MediaCert TSP during a security meeting of the MediaCert Committee. After approval, they are published and communicated to employees and third parties as necessary (see chapter 5.3.1).

All these documents are also subject to a revision process. This review process is triggered after each major addition or change of a Trusted Service and at least annually. The review process is the responsibility of the MediaCert Committee.

The Information System Security Policy (ISSP or ISP) applied by MediaCert TSP is managed (writing, revision, approval, publication) by the Worldline France Security Committee (see chapter 5.5). In addition, any significant change in the said ISSP resulting in a change in this GP will trigger a notification to the ANSSI (see chapter 5.3.1).

5.1.2 Point of contact

The authorized contact point for any comments, requests for additional information, complaints or dispute files, particularly concerning the MediaCert TSP's documentation is:

Comité MediaCert
Worldline
23 rue de la Pointe
Zone Industrielle A
59113 SECLIN
France
dl-mediacert-tsp@worldline.com

5.1.3 Entity determining the compliance of a practice statement with its associated policy

The consistency of a statement of practices with its associated policy is determined by the MediaCert Committee when validating the policy.

The consistency of technical documentation with the associated policy is determined by the MediaCert Committee when validating the policy.

5.1.4 Procedure for approving the conformity of a statement of practices with its associated policy

The process of verifying the compliance of a practices statement with the associated policy is guaranteed by the uniqueness of the document. The MediaCert Committee reviews and validates any major changes (see chapter 6.7).
The MediaCert Committee is responsible for the implementation and effective application of the practices described.

The compliance of a technical documentation with the associated policy - statement of practices is guaranteed by the writer of the technical documentation. Indeed, any modification of a technical documentation is made in parallel with the policy - declaration of practices concerned. The MediaCert Committee reviews and validates any major changes (see chapter 6.7).

In the event of a significant change in the provision of its qualified Trust Services, the MediaCert TSP shall inform the ANSSI in accordance with the procedures recommended by the latter within [ANSSI Qualification]. In particular in the following cases (not limited):

- changes induced by a change in the service policy or associated terms and conditions of use;
- changes in subcontractors;
- changes in accommodation conditions;
- changes in cryptographic equipment;
- changes in technical architecture;
- changes in registration and identification procedures;
- changes in the governance of MediaCert TSP's Trust Services.

Changes leading to changes in the trust list published by ANSSI are also notified as soon as possible.
In addition, the MediaCert TSP sends ANSSI a summary of all the changes made to the provision of its qualified Trust Services, impacting the findings presented in the conformity assessment report, on an annual basis.

5.2 Provision of information

5.2.1 Entity responsible for making information available

The MediaCert Committee is the entity responsible for making available the information to be published.

5.2.2 Information to be made available

The definition of the information to be published is specific to each Trust Service and is therefore available in the policies specific to the various Trust Services.

However, some elements are necessarily published on the site specified in chapter 5.2.3:

- the present General Policy, common to all Trust Services;
- the Terms and Conditions of each of the Trust Services.

The Terms and Conditions of a Trusted Service are made available to Users and Subscribers before any use of the service.

5.2.3 Place of availability of information

The information to be published is available on the MediaCert TSP's website, available 7 days a week, 24 hours a day, at https://www.mediacert.com
This website aims at a high availability requirement.

5.2.4 Time limits and frequency of publication

The deadlines and frequencies for publishing information are specific to each MediaCert TSP's Trust Service and are therefore available in the relevant policies, - except for documentation that must be published immediately, independently of the relevant Trust Service.

It is specified that the previous versions of the contractual documents (policies, general conditions, etc.) exclusively govern the periods of time covered by these versions, i.e. until their replacement notified to Subscribers. Indeed, as soon as a new version is notified to Subscribers and published, it will be immediately applicable for the future, the changes that have occurred concerning only editorial clarifications, changes related to the state of the art and regulations, without affecting the clauses of the contract between the Subscriber and MediaCert TSP but necessary for the qualitative monitoring of trust services. If, however, they should have an impact on the economy of the contract between the Subscriber and MediaCert TSP, the parties shall refer to the terms and conditions provided for in the applicable general conditions.

5.2.5 Access control to the information made available

All the information published on the MediaCert TSP's website is accessible to reading users. In addition, documents filed on this website are electronically signed to certify their authenticity.

Access to the information published on the MediaCert TSP's website for modification purposes is strictly limited to the authorized internal administrative functions. Access control is performed by servers dedicated to this function.

In addition, additional measures specific to Trust Services may be implemented, as defined in the following sub-chapters.

5.2.5.1 Certification Services

Access to the systems for publishing information on the status of Certificates (addition, deletion, modification of published information) is strictly limited to the authorized functions of the MediaCert TSP and is carried out through strong authentication on servers dedicated to access control.

5.2.5.2 Time-stamping services

Time Stamping Services are not subject to any additional measures other than those described in chapter 5.2.5.

5.2.5.3 Archiving Services

Archiving Services are not subject to any additional measures other than those described in chapter 5.2.5.

5.3 Amendments to the GP, CP-CPS, TP-TPS and AP

5.3.1 Amendment procedures

The MediaCert Committee regularly reviews the documents for which it is responsible.

When one of these documents is amended, it is generally reviewed and validated. The approval of the amendment is the responsibility of the Head of the MediaCert TSP, who does not make any documentary changes. The whole package the above-mentioned actions is carried out during a meeting of the MediaCert Committee. The Subscribers and Users concerned are notified in advance of the amendments by the MediaCert Committee members.

However, amendments to the revised documents are not always necessary. Indeed, changes in form (spelling, etc.) or editorial clarifications are not subject to validation and documents subject to prior notification to Subscribers and Users can then be updated without notification being made.

In the event of a major change in these documents, the following entities may also be notified of the change:

- the body in charge of conformity assessment;
- ANSSI, as the national control body for Trust Services;
- the SIAF, as the national control body for the archives of France.

5.3.2 OID Management

5.3.2.1 Construction of the OID

The OID of the MediaCert TSP's documents is based on the OID "**1.2.250.1.111**" assigned by AFNOR to Worldline and is constructed as follows: 1.2.250.1.111**.x.y.z.w** where:

- **x**: Worldline activity. Here it is the MediaCert TSP (Trust Service Provider → 20);
- **y:** number assigned to the policy of the relevant Trust Service;
- **z :** major version number of the document version (e.g.: v3.1 → 3) ;
- **w:** specific to each Trust Service.

5.3.2.2 Circumstances under which the OID must be changed

If the MediaCert Committee considers that a change in these documents has an impact on the level of security or trust in the relevant Trust Service, it may define a new version of the document and then assign it a new OID.

If the OID of this document is likely to evolve, the MediaCert Committee will take this evolution into account within the reference documents (CP-CPS, TP-TPS, AP, etc.).

5.4 Technical Documentation of General Practices

MediaCert TSP has a Technical Documentation of General Practices for its own use. This document details the security and legal measures common to the various Trust Services implemented by Worldline. These measures can be organizational, functional or technical.

5.5 Applicable information security policies

The measures defined in the Worldline Information Security Policy are applied within the scope of MediaCert TSP during all phases of its life cycle. This policy defines the objectives regarding the availability, integrity and confidentiality of information through a series of security rules. It demonstrates Worldline commitment to information security. It should be considered as a reference for all safety decisions. This is based in particular on recognized safety standards such as the [ISO 27001] standard and the ANSSI IT hygiene guide [Hygiene] for the standard level.

Information security measures specific to each Trust Service may be defined in the relevant technical documentation to meet their specific security needs.

The MediaCert TSP ensures that the Worldline ISP is documented and maintained by Worldline and implemented within the scope of all Trust Services. This includes responsibility for implementing security controls and operational procedures for all sites, systems, information and assets involved in providing the Trusted Service. The Worldline ISP is published and communicated to all employees affected by its scope.

The MediaCert Committee is responsible for the proper application of the Worldline ISP on all Trust Services. In particular, the MediaCert Committee ensures that it is properly applied even in the event of outsourcing a function of a Trust Service to a third party. To this end, in the event of subcontracting, the MediaCert TSP defines, where applicable, the responsibilities of its subcontractors and ensures that subcontractors comply with all the necessary controls (see chapter 6.6) and the obligation to train its employees (see chapters 7.3 and 7.4).

The security measures applied to the Trust Services are defined and validated by the MediaCert Committee. They are reviewed regularly and in the event of major changes, in particular in the event of changes that have a potential impact on the compliance, adequacy or effectiveness of the service. Any change affecting the level of security must be approved by the MediaCert Committee.

6 Organization of the management of Trust Services

6.1 Functions and responsibilities related to Trust Services

The MediaCert TSP explicitly defines the trusted roles required to ensure its operation and security. Definitions of trusted roles are made available to all staff concerned.
The functions performed on all components of MediaCert TSP's services are distributed among several types of stakeholders to ensure the separation of knowledge for sensitive tasks or roles. The trusted roles involved in the organization of MediaCert TSP are as follows:

- HSM Administrator: he is in charge of the installations and configurations of the cryptographic modules (HSM) of the MediaCert TSP;
- System administrator: he is in charge of the installation, configuration and maintenance of MediaCert TSP's trusted systems for service management. He is authorized to restore these systems; he also acts as a system operator, being responsible for the daily operation of MediaCert TSP's trusted systems.
- System auditor: he is authorized to consult the archives and all event logs of the MediaCert TSP's trust systems;
- Master of Ceremonies: he is in charge of managing the preparation and conduct of key ceremonies;
- Security Officer: he is in charge of administering the implementation of security practices and applying the technical constraints defined in the risk analysis;
- Registration operator: he is in charge of intervening in the process of creating Certificates;
- Secret carrier: he ensures the confidentiality, integrity and availability of secrets. It is the custodian of the secrets and physical keys to access their safes. He is a member of a team whose members all have the same rights to access the vaults;
- Application manager: he is in charge of monitoring the service and its performance. He coordinates and/or carries out the corrective and evolutionary maintenance of the application;
- Head of MediaCert TSP: he is in charge of the implementation of this GP, CP-CPS and TP-TPS as well as the verification of their application. In particular, he is in charge of revoking a Certificate issued by the CAs of the MediaCert TSP. As a member of the MediaCert Committee, he is also in charge of approving this document, policies (CP-CPS, TP-TPS and AP) and risk analyses of the MediaCert TSP;
- Deputy Head of MediaCert TSP: he is in charge of the same functions supported by the Head of MediaCert TSP;
- Security manager: he is in charge of defining the security rules around the MediaCert TSP.

When a new member is enrolled in a trusted role within the MediaCert TSP, a document acknowledging his or her appointment must be signed by the person concerned, for acceptance of the role, by the human resources manager and by the person in charge of the MediaCert TSP or one of his or her assistants. This document refers to the TDGP so that the future trusted staff member is aware of the description of his role and the responsibilities assigned to him. In particular, it specifies:

- the signatory's commitments and their proper understanding;
- in the event of a change in the TDGP document, the signatory will be informed.

Similarly, when a trusted role within the MediaCert TSP is terminated, a document recording the termination must be signed by the person concerned.

6.2 Number of people required

6.2.1 Number of people required per task

Depending on the type of operation performed, the number and roles of people to be present, as actors or witnesses, may be different. Indeed, some sensitive tasks, such as the generation of a CA's Certificate, require more than one person in a trusted role within the MediaCert TSP for security reasons.

6.2.2 Number of people required per role

Some trusted roles are held by several people so that MediaCert TSP can ensure the continuity of its services without compromising the security of the services offered.

It is regularly checked that all the trusted roles defined above are filled.

6.3 Identification and authentication for each role

Each staff in a trusted role is clearly identified by the MediaCert TSP through a role inventory.

Each entity operating a component of a MediaCert TSP's service checks, for each of its components, the identity and authorizations of any staff member as well as any external persons involved in sensitive tasks.

Before using a critical application contributing to a Trusted Service, all personnel must be identified and authenticated in advance. All operations carried out on the systems by staff are traceable (see chapter 12.5) guarantee the accountability of actions.

Each assignment of a trusted role to a MediaCert TSP's staff member is notified and documented in writing.

6.4 Separation of roles

It is hereby authorized by this GP that several roles be performed by the same person. However, as part of MediaCert TSP's activities and for security reasons, some roles cannot be performed by the same person. The separation of the roles identified above is specified in the TDGP.
In general, roles and responsibilities are assigned on the principle of least privilege in order to limit the risk of conflict of interest and limit the opportunities for unauthorized actions or misuse of assets implemented by the Trust Service.

6.5 Relations with the authorities

Relations with legal and regulatory authorities are ensured by the managers of the MediaCert TSP as defined in chapter 6.1 of this document, relying if necessary on the various appropriate departments of Worldline (administrative and legal department, etc.).

In particular, they are responsible for notifying the competent authorities in the event of a security incident as specified in the TDGP.

6.6 Relations with suppliers

The Worldline ISP defines the measures to be applied to suppliers in order to guarantee the application of a level of security at least equivalent to that defined in the ISP Worldline, for the activities entrusted to them. The measures integrate the concepts of training and control.

Relations with external suppliers are systematically formalized through a contractual agreement with the supplier. This agreement specifies the responsibilities of each party.

In any event, the MediaCert TSP, upstream, assesses the specific risks of outsourcing (information system control, remote actions, shared hosting, etc.) in order to take into account, as soon as the requirements applicable to the future service provider are drafted, the adapted security needs and measures.
MediaCert TSP requires its external service providers to have a security assurance plan (SAP) that formalizes its commitments or imposes appropriate security requirements in the service contract.

6.7 Governance bodies

The MediaCert TSP sets up a single governance body called the "MediaCert Committee" whose missions are multiple (validation of documentation, review of risk analyses, etc.). The people present at the meetings of this committee differ according to the subject of the meeting. However, the person in charge of the MediaCert TSP, or one of his deputies, is systematically present. Details are available within the associated TDGP.

6.8 Independence of the parties and non-discrimination

The organization set up within the framework of the MediaCert TSP, dedicated to its activities with a watertight role, makes it possible to preserve the impartiality of operations. In addition, the MediaCert TSP ensures that the trust activities provided are carried out in an equivalent manner for all beneficiaries who have accepted the terms of service and comply with their obligations.

To the extent possible, MediaCert TSP will implement appropriate approaches to make its service accessible to any person with a disability, taking into account on a case-by-case basis the specificities of each applicant.

Generally speaking, the services provided by MediaCert TSP such as the generation of Certificates, the management of Certificate revocation, electronic archiving or the issuance of Time-stamps are performed independently and are therefore not subject to any possible commercial pressure that could harm the ethics and professional conduct of these trusted services provided by MediaCert TSP. This is guaranteed by the fact that the MediaCert TSP is centralized within a *Global Business Line, a* unit that is transversal to the other units of Worldline (see Figure 2 - Organizational diagram).

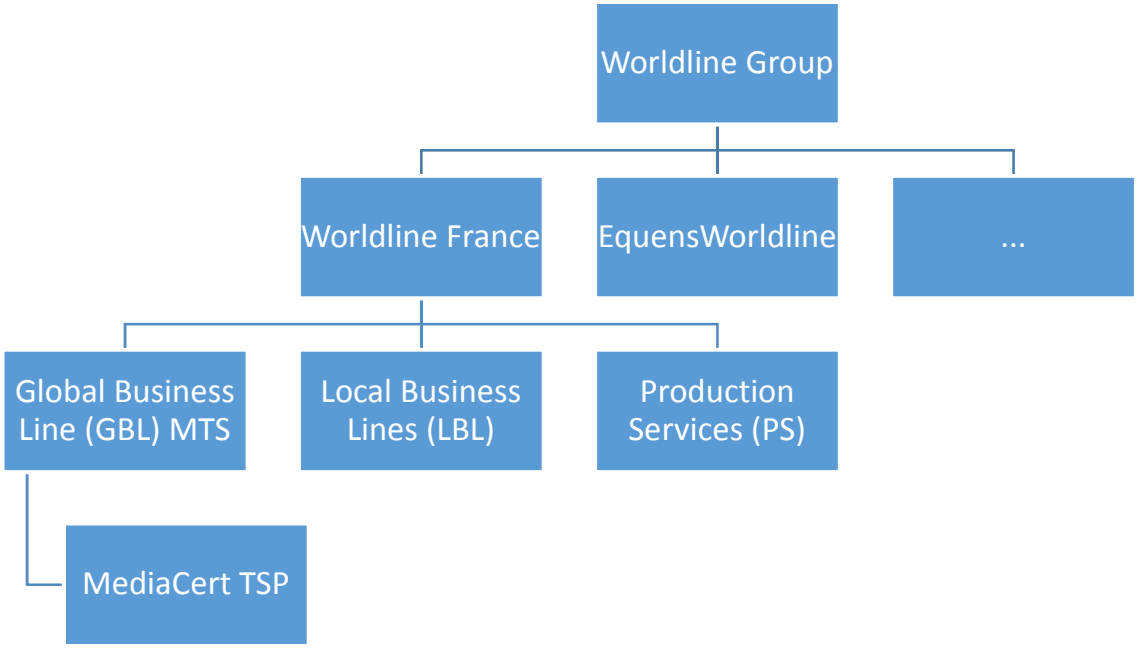

Figure 2 - Organizational diagram

7 Human Resources Security

MediaCert TSP implements a human resources policy that contributes to trust in the operations of the trust service. In particular, the MediaCert TSP implements the legal means at its disposal to ensure the honesty of the personnel impacting the trust services.

In addition, rights and access to the information system are updated according to staff changes (arrival, departure, change of affection). In particular, all the rights assigned to a person are revoked upon his departure or in the event of a change of function. Arrival and departure procedures are defined in conjunction with the human resources function. They take into account:

- the creation and deletion of computer accounts and associated mailboxes;
- the rights and access to be granted and withdrawn to a person whose function changes;
- management of physical access to the premises (allocation, return of badges and keys, etc.);
- the assignment of mobile equipment (laptop, USB key, hard disk, smartphone, etc.);
- the management of sensitive documents and information (transfer of passwords, change of passwords or codes on existing systems).

These procedures are formalized.

7.1 Required qualifications, skills and authorizations

MediaCert TSP employs staff and, where applicable, suppliers with the experience, skills, qualifications and expertise necessary to operate a Trusted Service.

Staff operating in trusted roles within the MediaCert TSP is informed of their responsibilities and the procedures related to system security and staff control with which they must comply.

Management personnel are trained and aware of security and risk management, are familiar with the security procedures in place and have sufficient IT security experience to fully assume their responsibilities for the services provided by MediaCert TSP.
Administrative and personnel management procedures are designed and maintained in line with information security management procedures.

MediaCert TSP ensures the qualification and competence of its staff operating in a trusted role.

7.2 Background check procedures

Criminal record check procedures are in place for individuals who are called upon to take on a trusted role within the MediaCert TSP. In particular, these persons must not have been convicted by a court of any offence likely to compromise their participation in the activities of the MediaCert TSP, nor be in a conflict of interest with their duties. In France, for example, the persons concerned must provide a copy of their criminal record bulletin No. 3 to Worldline Human Resources when signing the document (see chapter 6.1) in which they accept their role, obligations and responsibilities in connection with their participation in these activities. In particular, persons acting in a trusted role on behalf of TSP MediaCert are responsible for communicating any changes in this area. However, the MediaCert TSP sets up a regular verification of the adequacy of its members' criminal records with the role they operate on its behalf.

The candidate's application file is submitted to the Human Resources department for validation and to the Head of MediaCert TSP (see chapter 6.3). No access rights are granted until the file is validated.

The staff responsible for operating the MediaCert TSP's trust services are not responsible for the commercial aspects of these services and are free from any conflict of interest that could influence the way in which the operations for which they are responsible are conducted and undermine trust (see chapter 6.8). In this respect, they undertake to confirm in writing, upon acceptance of the trusted role within the MediaCert TSP, the absence of any conflict of interest related to the exercise of this new activity.
Any staff with a situation known to MediaCert TSP that could create a conflict of interest deemed incompatible or that could prejudice the impartiality of trusted service operations:

- cannot be assigned a role of trust;
- may be removed from a previously assigned trusted role.

7.3 Initial training requirements

Staff is trained in the software, hardware and operating procedures of the MediaCert TSP. He is also aware of information security and in particular:

- to safety issues;
- the rules to be respected;
- the right behaviour to adopt in terms of information system security.

This staff has taken the measure and knowledge of what is involved in the operations for which they are responsible.

All trusted personnel receive training typically concerning:

- security and protection of personal data;
- the legislation in force;
- the main risks and threats;
- the maintenance in a safe condition;
- authentication and access control;
- the fine configuration and hardening of the systems;
- network partitioning;
- logging.

This training may be adapted according to the department and the position held. It can take the form of theoretical training, practical training through the support of trained staff or a combination of both.

7.4 Continuing education requirements and frequencies

Staff shall receive the necessary training prior to any changes in systems, procedures, organization or others depending on the nature of these changes. In particular, he is trained on information system security issues and made aware of incident handling.

In particular, people receive regular training to maintain their level of expertise, knowledge and qualifications.

In addition, awareness-raising actions aimed at all employees are regularly implemented. These cover topics such as:

- the objectives and challenges that MediaCert TSP is facing in terms of information systems security (new threats and current security practices);
- information considered sensitive;
- regulations and legal obligations;
- the security rules and instructions governing the daily activity: compliance with the security policy, non-connection of personal equipment to the entity's network, non-disclosure of passwords to a third party, non-use of professional passwords in the private sphere and vice versa, reporting suspicious events, etc.;
- means available and contributing to the security of the system: systematic locking of the session when the user leaves his workstation, password protection tool, etc.

7.5 Frequency and sequence of rotation between different allocations

There is no defined rotation within this GL between the different allocations.

7.6 Sanctions in the event of unauthorized actions

Worldline internal rules state that appropriate administrative disciplinary sanctions are applicable in the event of misconduct (non-compliance with this GP, etc.). In particular, staff is reminded of this in the commitment of responsibilities they accept when accepting their role within the MediaCert TSP.

Entities outside Worldline and participating in the activities of MediaCert TSP are subject to sanctions defined during the contractualization in the event of misconduct (non-compliance with this GP, etc.).

7.7 Requirements for the staff of external service providers

The staff of any external service providers working on the premises and/or components of the MediaCert TSP must comply with the requirements set out in chapters 7.1 to 7.4 this document.

7.8 Documentation provided to staff

At a minimum, each person has documentation relating to the operational procedures and specific tools they implement, as well as the general policies and practices of the component of the service in which they work.

8 Asset Management

8.1 Asset Responsibilities

In accordance with the rules defined in the Worldline ISP, the MediaCert TSP:

- regularly inventories all the assets of the Trust Services it provides;
- designates an owner/responsible for the assets concerned.

8.2 Classification of information

MediaCert TSP's data is classified according to the Worldline Data Classification Policy. In addition, it follows the rules for handling information according to its sensitivity as defined in Worldline Information Protection Standard.

This classification of information is derived from the risk analysis and is maintained in accordance with its results (see chapter 4).

This classification makes it possible to implement an adequate level of protection. All assets are handled in accordance with this information classification document and associated procedures. In particular, end-of-life measures are put in place so that end-of-life assets containing sensitive information can be safely destroyed or decommissioned (see chapter 11.5).

9 Access control

9.1 Physical access

The sites and premises hosting MediaCert TSP guarantee the physical security of the means implemented to provide the Trusted Services. All the means put in place to ensure this are specified in the TDGP.

Physical access control measures are put in place to ensure that critical trust service systems cannot be accessed by unauthorized persons. These controls minimize the risks associated with the physical security of assets. In particular:

- critical[1] components are isolated within clearly defined security perimeters and are only accessible to authorized persons;
- security perimeters are subject to physical intrusion protection measures, access control measures and intrusion alarms;
- measures are in place to prevent theft, destruction or compromise of components, as well as service interruption;
- measures are in place against the compromise or theft of sensitive information;
- measures are in place to prevent equipment, information, media and software relating to MediaCert TSP's services from being removed from the site without authorization.

9.2 Logical access

Logical access to MediaCert TSP's servers, collaborative development tools and applications is monitored and regularly verified (see chapter 9.4).

9.3 Network access

Network access control measures are presented in chapter 13.1 this document. In particular, connections of personal equipment are prohibited on the MediaCert TSP network.

9.4 Management of access rights

The MediaCert TSP sets up a management of access rights on the basis of the principle of least privilege and regularly reviews the allocation of these access rights.

This management of access rights to MediaCert TSP's systems and information is internal and is specified in the TDGP document.

9.5 Manage accounts, passwords and sessions

[1] Criticality is defined by the classification of the information derived from the risk analysis.

Account management rules, passwords and access sessions to MediaCert TSP’s systems are in place to ensure minimum robustness of identification information and minimum protection of system access.

These rules are internal and are specified in the TDGP document.

10 Cryptographic measurements

Appropriate security measures and control procedures are in place for the management of cryptographic keys and cryptographic modules (HSMs) throughout their life cycle.

10.1 Standards and security measures for cryptographic modules

The HSMs used by the MediaCert TSP, for the generation of CA Key pairs, TSU Key pairs and those corresponding to the different Certificates issued by the CAs, are HSMs that meet the requirements defined in the policies associated with each relevant trust service.

These HSMs are dedicated to the services provided by MediaCert TSP.

MediaCert TSP ensures the safety of the HSMs it uses throughout their life cycle. In particular, procedures are in place to:

- ensure the integrity of these HSMs during transport;
- ensure the integrity of these HSMs during storage;
- ensure the integrity of these HSMs during their operation;
- ensure the proper functioning of these HSMs.

For qualified services within the meaning of the eIDAS Regulations, MediaCert TSP uses only HSMs that have been qualified at the level reinforced by ANSSI.

10.2 Key pair management

10.2.1 Key pair generations

10.2.1.1 CA and TSU key pairs

The generation of the CA or TSU Key pairs is carried out during a Key Ceremony. These key ceremonies are taking place:

- using a physically isolated HSM that meets the requirements defined in chapter 10.1 this document;
- in the secure premises of the MediaCert TSP (see chapter 11);
- under the permanent control of at least two (2) persons occupying a trusted role within the MediaCert TSP among: the secret holder, the master of ceremonies, the HSM administrator and the application manager (see chapter 6.1);
- according to an organizational document and a technical document, both signed by all participants, in particular by the master of ceremonies.

The private key of each CA and TSU is implemented and remains in the secure premises of MediaCert TSP.

10.2.1.2 Authentication keys for a component of a MediaCert TSP's service

The Authentication Keys of a component of a MediaCert TSP's service are generated during a Key Ceremony. This can be done at the same time as for CA or TSU keys. This ceremony takes place under the same conditions as those described in chapter 10.2.1.1 above.

10.2.1.3 Others

Each MediaCert TSP's service can define its own requirements in terms of key pair generation for other uses in accordance with applicable cryptographic requirements.

10.2.2 Transmission of the public key to users

The means of transmitting the public key to Users is specific to each service of the MediaCert TSP. This information is therefore found in the policies associated with each trusted service.

10.2.3 Key pairs size and algorithm

The size of the Key pairs and the algorithms used by the MediaCert TSP comply with the requirements [ETSI 119 312], the requirements [RGS B1] and the ANSSI [SOGIS_CRYPTO] recommendations.

10.2.4 Checking the private key

The control of CA private keys, corresponding backup copies and TSUs private keys is carried out by trusted personnel: secret holders and HSM administrators (see chapter 6.1); in a protected environment. This control is carried out using activation data, called "secrets", distributed among several persons identified in the role of secret carrier.

10.2.5 Private key escrow

MediaCert TSP does not offer a private key escrow service for collection purposes.

10.2.6 Backup copy of the private key

This operation is carried out under the control of several people during a Key Ceremony. Indeed, the backups of private keys are performed under the same conditions as those presented in chapter 10.2.1.1.

Backup procedures are performed according to the specifications of the MediaCert TSP's HSM provider.

The number of copies is limited to the minimum required to ensure the continuity of MediaCert TSP's services.

10.2.7 Archiving the private key

MediaCert TSP does not offer a private key archiving service.

10.2.8 Transfer of the private key to/from the cryptographic module

CA private keys are generated within an HSM (see chapter 10.2.1.1) and are only transferred to another HSM in the case of backup copies (see chapter 10.2.6).

During a transfer, the private key is encrypted with an algorithm recommended by the HSM manufacturer to ensure information security. The encrypted private key cannot then be decrypted without the use of hardware cryptographic components and the action of identified persons in the necessary trusted roles.

10.2.9 Storage of the private key

CA and TSU private keys are stored in a physically secure HSM that meets the requirements defined in chapter 10.1 this document. The same applies to the storage of backup copies of CA private keys.

Procedures around these HSMs are in place to ensure the confidentiality of their content.

10.2.10 Method of activating the private key

CA private keys can only be activated with activation data held by two (2) persons in a trusted role within the MediaCert TSP.

The activation of a CA private key can only be done during a documented and traced Key Ceremony.

10.2.11 Method of deactivating the private key

The deactivation of CA private keys in the HSM is automatic as soon as it is stopped.

10.2.12 Method of destroying private keys

CA private keys, corresponding backup copies and TSUs private keys shall be deleted from the cryptographic resource in accordance with the manufacturer's procedures. The destruction operations are carried out during an audited procedure such as Key Ceremony.

At the end of its normal or anticipated life (due to revocation) of a private CA or TSU key, it is systematically destroyed, as well as any copy and any element allowing it to be reconstituted. In addition, if the hardware cryptographic resource hosting the above-mentioned private keys must be decommissioned, then so must they.

10.3 CA private key activation data

10.3.1 Generation and installation

CA private key activation data is generated in an HSM during key ceremonies under the control of two (2) people in trusted roles, stored on smart cards and then given to secret holders who then hold the activation data. These activation data are only known by those responsible who are identified by name in the context of the trusted role assigned to them.

10.3.2 Protection

Activation data is protected by cryptographic and physical access control mechanisms. Secret bearers are responsible for protecting the secrets for which they are responsible. A bearer of a secret does not hold more than one activation data per CA.

11 Physical and environmental security

A set of physical security measures is put in place by MediaCert TSP to ensure that:

- the means, information systems and data used in the operational implementation of the MediaCert TSP are installed in secure premises, access to which is controlled and restricted to strictly authorized personnel. The physical access control system makes it possible to guarantee the nominative traceability of access to the premises hosting the means and information of the MediaCert TSP (cf. chapter 9.1);

- the implementation of these controls makes it possible to respect the separation of trusted roles as provided for in this GP (see chapter 6.4).

Below is a list of environmental measures implemented to ensure the availability of hosted equipment and the continuity of services provided by MediaCert TSP. Details are provided in the TDGP document.

11.1 Geographical location and site construction

MediaCert TSP’s environments are installed on secure Worldline European IT production sites. These sites are designed to host IT and telecom systems.
MediaCert TSP's administrative and operational teams operate on European Worldline sites.

11.2 Power supply and air conditioning

A number of measures (emergency generators, etc.) are in place to prevent power failures and simplify maintenance operations. Similarly, measures (system redundancy, etc.) are put in place to prevent failures in the air conditioning system. These preventive measures are regularly maintained and tested.

11.3 Vulnerability to water damage

Monitoring means (sensors, monitoring, etc.) are in place to prevent water damage. These monitoring systems are regularly maintained and tested.

11.4 Fire prevention and protection

Fire prevention and control measures (detectors, fire doors, etc.) are in place to prevent any risk of fire and to protect MediaCert TSP’s systems if necessary. These preventive and protective measures are regularly maintained and tested.

11.5 Decommissioning of supports

All paper documents containing confidential data (PIN code, password, etc.) that are no longer needed or obsolete are physically destroyed.

For physical media (disc, HSM, etc.) a special buffer storage procedure for grinding is set up. This destruction gives rise to the production of a Minute.
In particular, if an HSM is deactivated, the 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.

12 Operational management

12.1 Computer system security measures

12.1.1 Technical security requirements specific to computer systems

The minimum technical security requirements implemented by MediaCert TSP meet the following objectives:

- strong user identification and authentication for system access (see chapter 9.2);
- protection of the network against unauthorized access (see chapter 9.3);
- management of user and account rights (see chapters 9.4 and 9.5);
- management of user sessions: disconnection after a period of inactivity, access to files controlled by role and user name (see chapter 9.5);
- audit functions: non-repudiation, accountability and nature of actions performed (see chapter 15);
- application of change procedures for delivery, modification and urgent resolution of software problems (see chapter 12.2);
- protection against viruses, malicious or unauthorized software and software updates (see chapter 12.3);
- application of change procedures for any modification of software configurations (see chapter 12.8);
- protection of the network to ensure the confidentiality and integrity of the data transmitted over it (see chapter 13);
- redundancy of network connections to ensure accessibility in the event of a simple failure.

Monitoring devices, with automatic recording and alarm, as well as procedures for auditing system settings, in particular routing elements, and incident response procedures are in place.

12.1.2 Qualification level of computer systems

MediaCert TSP uses reliable systems to store the data provided to it in a verifiable form so that:

- the data are only publicly available for processing after having obtained the consent of the person concerned by the data;
- only authorized persons may enter and modify the stored data;
- the authenticity of these data can be verified.

Details are provided where necessary in the policies associated with each service.

12.1.3 Handling and security of the supports

The media used by MediaCert TSP are handled securely, according to defined procedures, to protect them from damage, theft, unauthorized access and obsolescence.

The measures specifically address the reuse of media that have contained information in another context, so that it cannot be accessed by unauthorized persons.

Media containing sensitive data shall be disposed of in accordance with the definition in chapter 11.5 this document.

Backup media are subject to specific measures described in 12.4.1.

12.2 Operating procedures and responsibilities

The operating procedures of the MediaCert TSP are documented and made available to the concerned teams, in particular all administrative staff or staff in a trusted role that may have an impact on the provision of the Trusted Service.

In particular, change monitoring procedures are in place to control software deployments, updates and emergency fixes, as well as changes in system configurations involved in the provision of Trust Services. MediaCert TSP relies on an internal Worldline tool to track changes and incidents related to the operation of its services. The tool is used to document all changes made.

MediaCert TSP ensures that the different environments of the production environment are distinguished for all Trusted Services systems operated.

12.3 Protection against malware

MediaCert TSP implements a set of solutions to protect its production platforms and administration stations against viruses and malicious or unauthorized software. These solutions are specified in the TDGP.

12.4 Backups

12.4.1 Conservation of the supports

As part of MediaCert TSP's activities, backups of a different nature are performed. Measures are then put in place to ensure the availability, confidentiality and integrity of the backup media used. These measures are described in the TDGP. These measures may address, where appropriate, the problems of obsolescence and deterioration of media, in particular when it is necessary to keep data for long periods.

12.4.2 Off-site backups

As part of this GP, MediaCert TSP is implementing off-site backups in accordance with the procedures defined by Worldline.

12.5 Logging and monitoring

12.5.1 Logging

The logging measures implemented are described in chapter 15.1 this document.

12.5.2 Event log monitoring

Event logs are inspected when they are issued by tools specified in the TDGP. These tools make it possible, in particular, to automatically trigger alarms in order to notify the event manager of a potential incident detected, in particular a critical safety incident.

12.5.3 Capacity monitoring

A projection of future capacity requirements on MediaCert TSP's platforms is regularly carried out, usually at meetings organized by the MediaCert Committee. In particular, these platforms are monitored for capacity (availability and use of services) to ensure adequate processing and storage capacity.

12.5.4 Safety monitoring

A tool (SIEM) is implemented to process event logs (analysis, correlation) in order to identify and report security alerts. The MediaCert TSP relies in particular on a team dedicated to these activities (SOC) to report security alerts and thus meet the requirements to which it is subject.

In particular, the following events are monitored:

- stop and start of trace generation functions;
- abnormal activity on the network.

Alerts are processed by the TSP according to the procedures described in chapter 14.

A regular review is carried out with this team to review abnormal events and prevent configuration changes.

12.5.5 System monitoring

MediaCert TSP's systems are monitored using various tools to ensure that they are functioning properly.

12.6 Mastery of software in operation

MediaCert TSP masters the software (inventory, versions, etc.) installed on its systems. In addition, only the necessary software is installed on the systems in production. These software products have been selected for their reliability and ability to ensure the security and continuity of the services they provide. They are subject to security measures to protect them from any modifications or alterations.

Systems are hardened by removing unused accounts, applications, services, protocols and ports.

Installation rights on the various environments of the MediaCert TSP Trust Services are limited and subject to change procedures (see chapter 12.2).

12.7 Technical vulnerability management

The MediaCert TSP provides technical vulnerability management via:

- the implementation of patch management processes;
- the implementation of technical monitoring;
- of vulnerability scans.

These processes are available in the TDGP document.
These processes make it possible to detect potential vulnerabilities and create vulnerability correction plans in order to maintain the information system in optimal security conditions. It is possible that a vulnerability may not be the subject of a correction plan, however, the MediaCert TSP then documents the elements that justify this arbitration.

Any critical vulnerability must be addressed within forty-eight (48) hours of its discovery.
These processes also ensure that:

- patches are applied within a reasonable time after they are made available;
- patches are not applied if they introduce vulnerabilities or instabilities that offset their theoretical benefits;
- if a patch is not applied, the reasons for this decision are documented.

Vulnerability scans are performed on a regular basis by personnel with the skills, tools, ethics and independence necessary to produce a reliable report.

12.8 Acquisition, development and maintenance of information systems

The implementation, configuration and any modification or update of a system to implement the components of a MediaCert TSP service is documented and controlled (see chapter 12.6). Any changes that impact the security level must be approved by the MediaCert Committee.

Developments are made according to Worldline secure development policy. This covers design, development, testing and deployment in production. It is based on recognized good security practices. An analysis of security requirements is performed at the time of design or selection of each of the architecture components to ensure that security is taken into account in the IT systems.

MediaCert TSP does not use outsourced developments for trust services.

Developments are systematically passed into an automatic analysis tool to control the quality of the code.

Developments are subject to functional tests and acceptance before delivery to production.

Production data is not copied to pre-production, test or development environments. Anonymized test or data sets are used for tests and developments.

13 Communications Security

13.1 Network access management

MediaCert TSP is implementing measures to protect its network against possible attacks.

13.1.1 Network partitioning

MediaCert TSP's platforms are hosted in separate network areas depending on their role and sensitivity. Critical network components are maintained in a secure environment. The sensitivity of the various elements is established in line with the results of the risk analysis. MediaCert TSP applies the same security controls to all components in a network area.

In particular, network flows to the MediaCert TSP, as well as between each separate network area, are monitored (see chapter 13.2) in order to prevent any unauthorized flows (including flows from users or service subscribers). In particular, network control devices are configured to prohibit all protocols and access that are not necessary for trusted service operations.
Configurations are subject to regular review.

Production and test/development environments are also compartmentalized.

In order to document the partitioning, the MediaCert TSP creates and maintains a simplified network schema (or mapping) representing the different IP zones and the associated addressing plan, routing and security equipment (firewalls, application relays, etc.) and interconnections with the outside world (Internet, private networks, etc.) and partners. This scheme makes it possible to locate the servers holding the entity's sensitive information.

13.1.2 Access to platforms

MediaCert TSP’s platforms are subject to logical access restrictions (see chapter 9.3) and are not directly accessible. The process for logical access to MediaCert TSP’s platforms is internal and described in the TDGP. Access control management is under the control of MediaCert TSP. This management includes account management and allows you to modify or delete accesses without delay. Access rights and privileges to the platforms are assigned according to the logical access policy defined by the MediaCert TSP.

The access control system in place allows for efficient and adequate access management, in particular:

- it allows a separation of roles, in particular between administration operations and other business level operations by using networks dedicated to each of the uses;
- it allows you to control and restrict the use of different applications and utilities.

The systems used for administration are dedicated to this purpose.

Penetration tests are carried out when the service infrastructure is set up and then at each major change or modification. Due to their criticality, and the importance of providing a reliable report, penetration tests can only be performed by personnel selected on criteria such as their skills, knowledge, effectiveness, ethics and independence.

13.1.3 Access to services

MediaCert TSP’s services are not in direct contact with networks open to the Internet. The gateways allowing access are protected against intrusion or attack attempts.

These gateways limit open services and protocols to only those services essential to the operation of the services provided by MediaCert TSP. They are regularly updated to take into account developments in anti-intrusion systems and to close potential security gaps.

13.2 Information transfer

In the event that they are not located in a dedicated network, all communication flows between MediaCert TSP’s equipment are exclusively via secure network communication protocols that guarantee the confidentiality and integrity of the communication.

13.3 Redundancy

The external connection is redundant to provide a high level of service availability.

14 Incident management

In the event of an alert escalation, MediaCert TSP has set up an incident management system to respond in a coordinated and rapid manner to incidents in order to limit their impact.

14.1 Security incident management

Incident management processes are in place to limit the consequences of such incidents and to inform the parties concerned in a timely manner. In particular, the follow-up of alerts that may be linked to a security incident is carried out by staff in a role of trust. These personnel ensure that the reporting and processing of these incidents is carried out in accordance with the incident management procedures established by the MediaCert TSP.

In addition, in the event of compromise of the Trust Services, the competent legal authorities are notified if the nature of the compromise so requires. In particular, a proven security incident affecting the integrity of the trust service or compromising personal data must be reported within twenty-four (24) hours:

- to ANSSI in all cases, following the procedure recommended by ANSSI;
- to the CNIL in the event that the incident impact of personal data.

MediaCert TSP will also notify affected Subscribers.

These processes include the review of incidents to ensure the follow-up of corrective and preventive action plans to prevent recurrence of such incidents.

They also provide for the establishment of surveillance to detect security incidents as soon as possible (see chapter 12.5.4).

14.2 Security incident management procedures

Procedures are established to ensure an appropriate response to proposed incidents. To do this, MediaCert TSP relies on the Worldline Incident Management Policy, which deals in particular with the classification and reporting of security incidents. In this respect, the MediaCert TSP has its own notification procedure, described within the TDGP.

These procedures address, in particular, the case of compromise of Trust Services and service interruptions. In addition, in the event of corruption of IT resources or technical incidents, MediaCert TSP has implemented a Business Continuity and Resumption Plan for each of the trust services it provides (see chapter 16.2).

15 Collection of evidence

15.1 Logging

The events involved in the life of the MediaCert TSP are logged as files from software-automated generations and supplemented, if necessary, by manual entries. The purpose of these files is to ensure the traceability and accountability of the operations performed (authors, timestamps, etc.).

Event logs explicitly include the performer's identifier (software or human), the date and time of the operation and the nature of the event.

They may be made available to the courts upon a legal request by the applicants.

15.1.1 Type of events logged

The MediaCert TSP's logs related events:

- security (including access or attempted access);
- the activities and life cycle of the systems of the trust services it provides.

These event logs can be in electronic or handwritten form. All these events are listed in the TDGP technical documentation relating to this document.

15.1.2 Frequency of event log processing

The monitoring systems implemented (see chapter 12.5.2) process logs as soon as they are collected.

15.1.3 Frequency of storage of event logs

Event logs are exported over time to a remote server.

15.1.4 Event log retention period

Event logs are kept over different time periods depending on the type of event and the trust service involved. These retention periods are specified in the policies associated with the various trust services of MediaCert TSP.

15.1.5 Protection of event logs

Electronic event logs are collected via the system described in chapter 15.1.7 this document and then outsourced to two types of environment (supervision and notarization) whose administrations are different. Access to these elements is therefore only possible to personnel authorized by the MediaCert TSP as defined in the TDGP document and cannot be modified or deleted without authorization.

Handwritten event logs are protected by secure physical systems such as safes or strong cabinets whose accesses are controlled by the MediaCert TSP.
These systems ensure the integrity and confidentiality of event logs.

15.1.6 Procedure for backing up event logs

The procedure for backing up MediaCert TSP event logs is internal and is specified in the TDGP document.

15.1.7 Event log collection system

The MediaCert TSP's event log collection system is internal and is specified in the TDGP document. This takes into account the sensitivity of the information collected and analyzed.

15.1.8 Notification of the registration of an event to the event manager

There is no systematic notification of the recording of an event to the event manager.

15.2 Archiving

15.2.1 Protection of archives

The confidentiality of the archives is ensured by appropriate physical, system and network access management. It ensures the completeness and confidentiality of the archives.

During their period of retention in MediaCert TSP's secure premises, the archives are protected in integrity and are accessible only to authorized persons. Indeed, the request for access to an archive can only be made by the head of the MediaCert TSP, a deputy head of the MediaCert TSP or the security officer of the MediaCert TSP in order to ensure the confidentiality of the information.

Procedures are in place to prevent obsolescence and deterioration of the archives. In particular, they are stored in premises subject to measures to protect against natural threats.

15.2.2 Archive backup procedure

The level of archive protection is equivalent to the level of backup protection. Archive backup procedures are internal and are specified in the TDGP document.

15.2.3 Data time stamping requirements

All events are precisely dated with the system time of the MediaCert TSP servers. MediaCert TSP's servers synchronize their internal clock regularly (at least every 24 hours) on reference servers to ensure the consistency of the time (UTC) indicated in the various electronic logs.

15.2.4 Archive collection system

The MediaCert TSP's event archive collection system is internal and is specified in the TDGP document.

15.2.5 Procedure for retrieving and verifying archives

The archives may be retrieved within a period of less than two (2) working days from the registration of the request. Access to the archives is subject to restrictions (see chapter 15.2.1).

The archives will be made available in case of judicial requisition.

16 Business continuity

16.1 Availability commitments

The availability target for the MediaCert TSP's website is specified in chapter 5.2.3 this document.

In addition, MediaCert TSP has availability commitments specific to each trusted service it provides.

16.1.1 Certification Services

The Certificate status information function is available 7 days a week, 24 hours a day. MediaCert TSP aims for the lowest possible level of unavailability.

16.1.2 Time-stamping Services

The targeted availability for the provision of the service is defined within the relevant policy.

16.1.3 Archiving Services

The targeted availability for both the capture service and the archive consultation service is defined within the various archiving policies.

16.2 Business continuity and recovery

In the event of interruption or corruption of IT resources (hardware, software and/or data), in particular in the event of compromise of the private key of a component, the MediaCert TSP will then apply the Continuity and Business Resumption Plan of the concerned service in order to ensure the continuity and/or restoration of the service as soon as possible.
Remedial measures are put in place to limit the risk of a new incident occurring.

The IMP and BCP are regularly updated by Worldline security teams and the teams in charge of MediaCert TSP respectively.

17 End of activities

MediaCert TSP is implementing a business interruption plan to minimize the impact of a business interruption on Subscribers and Users.

In the event that MediaCert TSP decides to discontinue the provision of one of its trusted services, the termination plan of the service concerned will then be applied. Each of the plans for the termination of the trust services includes the following points:

- information of the decision of the MediaCert TSP to the persons concerned (supervisory bodies such as ANSSI, partners, Subscribers, users) before the termination of the service's activities, subject to prior notice;
- repeal of the authorizations given to potential subcontractors to act on its behalf in the performance of any functions related to the service provision process;
- transfer to Worldline of its obligations to maintain the event logs and archives necessary to demonstrate the correct operation of the service for a reasonable period of time;
- destruction of private keys (nominal and backed up) concerned by the service in such a way that they cannot be recovered;
- maintaining or transferring to Worldline its obligations to make its public keys and Certificates concerned by the User Service available for a reasonable period of time.

The termination plans of the various trust services of MediaCert TSP are regularly reviewed and updated in accordance with the state of the art.

In the event that MediaCert TSP goes bankrupt, it will cling to Worldline to cover the end-of-life obligations of the trust services it provides.

Each policy of a MediaCert TSP's Trust Service can complement these points with provisions specific to the type of trust service implemented.

18 Conformity

18.1 Insurance

18.1.1 Insurance coverage

Worldline has, with a company known to be solvent, an insurance policy guaranteeing the damage that may occur to its property, its staff, as well as a policy covering its professional liability in connection with the services provided.

18.1.2 Other resources

Worldline has the financial resources to provide the services of MediaCert TSP.

18.1.3 Coverage and guarantee for user entities

MediaCert TSP cannot be held responsible for any unauthorized or non-compliant use of the services it provides (Certificates, Time-stamps).
Indeed, MediaCert TSP can only be held liable in the event of proven non-compliance with its obligations.

In addition, to the extent of the limitations of the law, MediaCert TSP shall not be held liable:

- no financial loss;
- no data loss;
- any indirect damage related to the use of a Certificate or Time-stamps;
- of any other damage.

MediaCert TSP is generally not responsible for the documents and information provided by the Subscriber and does not guarantee their accuracy or the consequences of harmful facts, actions, negligence or omissions by the Subscriber.

In any event, the liability of MediaCert TSP shall be limited, for all events and for all damages combined, to the amount for access to the relevant trusted service as specified in particular in the associated service contract, in compliance with and within the limits of applicable law.

18.2 Confidentiality of professional data

18.2.1 Scope of confidential information

The following information is considered confidential:

- technical information relating to the safety of the operations of the HSMs and certain components of the MediaCert TSP’s services;
- private keys of CAs, their components and issued Certificates;
- the private keys of the TSUs;
- activation data of CA and TSU private keys;

- the technical documentation relating to the policies of the various trust services;
- internal operating procedures;
- the continuity and disaster recovery plan for the various trust services;
- the plan for the cessation of activity of the various trust services;
- registration files;
- audit reports.

Only persons authorized by Worldline and having the need or authorization to know its content may consult, upon request, the above-mentioned information. This request must be forwarded to the person in charge of the MediaCert TSP or one of his or her assistants.

18.2.2 Information outside the scope of confidential information

The information of the MediaCert TSP considered public and therefore non-confidential is as defined in chapter 5.2.2 this document.

18.2.3 Responsibility for the protection of confidential information

MediaCert TSP undertakes to treat confidential information collected in compliance with the laws and regulations in force.

18.3 Protection of personal data

18.3.1 Personal data protection policy

Worldline ensures the protection of the personal data it holds or is likely to hold, in accordance with the rules relating to the protection of personal data in force in the territory from which it provides its services.

These data are protected according to the French national law applicable to its services, which in France is in conformity with the European regulations both eIDAS and the GDPR (cf. chapter 18.7).

Thus, in accordance with the eIDAS Regulation, MediaCert TSP takes the appropriate technical and organizational measures to manage the security risks associated with the trust services it provides. Taking into account the latest technological developments, these measures shall ensure that the level of safety is proportionate to the degree of risk. In particular, measures shall be taken to prevent and limit the consequences of security incidents and to inform the parties concerned of the adverse effects of such incidents.

In the event of a breach of personal data, MediaCert TSP refers to the Worldline Personal Data Breach Handling Procedure made available to it.

MediaCert TSP acts in accordance with RCL type obligations (Regulatory and Contractual Legal).

18.3.2 Responsibility for the protection of personal data

Worldline processes personal data in accordance with the laws and regulations defined in chapter 18.7 this document, which are in line with those prevailing in Europe regarding the protection of personal data.

18.3.3 Right of access to data

In accordance with Article 40 of the Data Protection Act amended by Law No. 2016-1321 of 7 October 2016 - Art. 63, any natural person proving his identity may require the controller of a processing operation to rectify, complete, update, lock or delete, as the case may be, personal data concerning him, which are inaccurate, incomplete, ambiguous, outdated, or whose collection, use, communication or storage is prohibited. Where the data subject so requests, the controller must provide proof, at no cost to the applicant, that he or she has carried out the said operations.

The right of access may be exercised in writing: by post to the MediaCert TSP's contact point, at the address given in chapter 5.1.2 this document or on the MediaCert TSP's website (see chapter 5.2.3), accompanied by a copy of an identity document. Ideally, by registered mail with acknowledgement of receipt.

18.3.4 Conditions for disclosing personal information to judicial or administrative authorities

Worldline may have to make available personal information collected to authorized third parties in connection with legal proceedings or audits to verify the validity of the operation of MediaCert TSP's services. The latter has secure procedures to allow these accesses, which are tracked by name and stored.

18.4 Intellectual and industrial property rights

MediaCert TSP acts in accordance with the legislation and regulations defined in chapter 18.7 this document. Public documents, outside the scope of confidential information, remain the property of Worldline.

18.5 Provisions concerning conflict resolution

For any dispute, it is advisable to contact the MediaCert TSP at the contact point described in 5.1.2.
The parties shall endeavour to settle amicably any dispute concerning the interpretation or execution of the contract as soon as possible. In the absence of conciliation, any dispute relating to the validity, interpretation or execution of this General Policy, the Services Policies or the Terms and Conditions shall be submitted to the competent courts indicated in 18.6.

Additional dispute resolution provisions specific to each MediaCert TSP's Trusted Service may be set out in the policies and Terms and Conditions of those services. They are therefore defined in the associated policies and/or general conditions.

18.6 Competent jurisdictions

In the event of a dispute relating to the Trust Services provided by MediaCert TSP, including the related documentation and failure to reach an amicable agreement, any dispute will be brought before the competent courts in Paris.

18.7 Compliance with laws and regulations

The MediaCert TSP, in all its components and including documentaries, is governed by the French legislation and regulations applicable to it, itself generally based on European texts, although its activities resulting from this GP may have legal effects outside French territory.

A regular monitoring is carried out to verify compliance with these legal constraints.

In addition, only the French version of the contractual documents (including this GP) is enforceable against the parties, even in the presence of translations. Indeed, the translations of express agreements are provided for mere convenience and cannot have any legal effect, in particular on the interpretation of the Subscription Contract or the common intention of the parties.

18.8 Force majeure

Are considered as force majeure all those usually retained by the jurisprudence of French courts and tribunals, including the case of an irresistible, insurmountable and unpredictable event. As such, MediaCert TSP cannot be held liable for any indirect damage and interruption of its services due to force majeure.

18.9 Audits

MediaCert TSP subjects its services to compliance audits or other means of evaluation. Each department provides details on the subject within their specific policy.

18.9.1 Frequency and/or circumstances of evaluations

Worldline audits the compliance of its various trust services (Certification Service, Time-Stamping Service and Archiving Service) with current policies during the operational implementation of a component of a trust service and during any significant change within a component by an accredited organization.

Worldline may have to carry out a surveillance audit (internal or external) between two external certification audits to the standards in force on the trust service of the MediaCert TSP concerned.

18.9.2 Identities / qualifications of assessors

18.9.2.1 Certification audit

The audit of the trust service component is carried out by a team of auditors who are part of an audit body authorized and accredited to carry out assessments according to the specifications of the standards applicable to the trust service of the evaluated MediaCert TSP.

18.9.2.2 Surveillance audit

The control of the trust service component is performed by a compliance control team that is independent of the evaluated MediaCert TSP trust service.

18.9.3 Relations between evaluators and evaluated entities

18.9.3.1 Certification audit

The evaluator(s) carrying out the audit of the component(s) of the trusted service being appraised shall be independent and free of any conflict of interest.

18.9.3.2 Surveillance audit

The evaluator(s) performing the audit of the component(s) of the trusted service being evaluated do not have any trusted role within the MediaCert TSP.

18.9.4 Topics covered by the evaluations

The audits carried out by the auditors cover some or all of the components of a MediaCert TSP trust service in order to monitor compliance with the implementation of this GP and the compliance of the trust service's procedures and practices with the requirements to which it is subject.

In this respect, before each audit, the evaluator responsible for the audit sends the MediaCert TSP an audit plan, specifying the components and procedures that he will wish to audit during the audit with his colleague(s) as well as the detailed audit program.

18.9.5 Actions taken in response to evaluation findings

Following an evaluation, the audit team provides Worldline with its opinion on the following options:

- Success: the audit found no non-compliance and no further action is required. Worldline confirms the compliance of the audited component with the commitments in this document and the practices announced;
- to be confirmed: the audit identified one or more non-blocking non-conformities. Worldline must then present a corrective action plan with a deadline for completion. A new check may be carried out to verify the implementation of the corrections;
- failure: the audit found one or more blocking non-conformities. The audit team then makes recommendations to Worldline, which may include temporary or permanent cessation of activity, etc. The choice of the measure to be applied is up to Worldline.

18.9.6 Communication of results

The results of the compliance audits are made available to the audit body in charge of certifying the trust service of the evaluated MediaCert TSP.