TSL Policy for EPC e-Mandates e-Operating Model

Policy

MULTICERT_PJ.EPC_24_0001_en

Project Identification: EPC-TSL

Rating: Public

Version: 2.0

Date: 2014-07-01

Document Identification: MULTICERT_PJ.EPC_24_0001_en

Keywords: EPC TSL Policy e-Operating Model e-Mandates SEPA PKI Certification Authorities CA direct debits

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edifício 3, Piso 3, 2740-266 Porto Salvo, Oeiras, Portugal
Phone: +351 217 123 010 Facsimile: +351 217 123 011

Document Type: Policy

Title: TSL Policy for EPC e-Mandates e-Operating Model

Original Language: English

Language of Publication: English

Rating: Public

Date: 2014-07-01

Current Version: 2.0

Project Identification: EPC-TSL

Client: EPC

Version History

Version Number	Date	Details	Author(s)
1.0	2012-08-31	Initial version	MULTICERT
1.1	2014-06-19	Address and logo update	MULTICERT
2.0	2014-07-02	Approved version	MULTICERT

Related Documents

Document Identification	Details	Author(s)

Executive Abstract

This document is provided as the policy applicable to the TSL supporting the EPC e-Mandates e-Operating Model [1], [2], [3], [4], [6]. It describes the constraints and conditions under which the TSL is maintained and offered.

Table of Contents

1 Introduction

The European Payments Council (EPC) Trusted-Service Status List (TSL) [7] is the trust anchor for Public Key Infrastructure (PKI) enabled applications based on the EPC e-Mandates e-Operating Model [1], [2], [3], [4], [6]. It is a publication of the X.509 certificates of all Certification Authorities (CA) approved to participate in protocols and frameworks built on top of the e-Operating Model.

This document is the policy applicable to the TSL supporting the EPC e-Mandates e-Operating Model [1], [2], [3], [4], [6]. It is the principal statement of policy governing the TSL. It describes the general practices and constraints followed by the scheme operator for the issuance and management of the TSL.

This document may be subject to further revisions in the future and shall follow the approval and notification procedures defined in section 1.5.4.

1.1 Overview

The decentralized PKI trust model adopted by the EPC for the e-Operating Model [1], [2], [3], [4], [6] requires harmonized security practices amongst the participating CAs in order to establish a global trusted anchor. Such trust anchor is the EPC TSL, an XML file compliant with ETSI 102 231 containing the information about the approved Certification Authorities, including the X.509 certificates [8], [9].

The EPC TSL is, thus, the primary source of trusted CAs that shall be accepted across participants in applications, services and frameworks built atop the EPC e-Mandates e-Operating Model [1], [2], [3], [4], [6].

1.2 Document Name and Identification

This document is called the "TSL Policy for EPC e-Mandates e-Operating Model" and is assigned the identifier MULTICERT_PJ.EPC_24_0001_en.

1.3 TSL Participants

The following entity types are participants within this TSL scheme:

- *TSL Promoter* – body responsible for establishing the initiative of this TSL and the underlying terms, rules, regulations and supervision. The operational responsibilities (in part or whole) are delegated to the TSL Scheme Operator. For this TSL, the promoter is the "European Payments Council (Conseil Européen des Paiements AISBL)"[1].
- *TSL Scheme Operator* – body responsible for operating, issuing, managing and publishing the TSL. For this TSL, the TSL Scheme Operator is "MULTICERT – Serviços de Certificação Electrónica

[1] http://www.europeanpaymentscouncil.eu

S.A."[2]. The terms "MULTICERT" and "TSL Scheme Operator" are used interchangeably throughout this document and refer to the same entity.

- *Certification Authorities* – Trust Service Providers operating Trust Services, which, for this TSL, must be Certification Authorities issuing X.509 certificates conforming to the EPC e-Mandates e-Operating Model Detailed Specifications 3. Approved CAs [5] are listed in the TSL and shall be trusted by all relying parties participating in applications, services and frameworks built atop the EPC e-Mandates e-Operating Model.
- *Subscribers* – bodies operating applications, services or frameworks built atop the EPC e-Mandates e-Operating Model and requiring X.509 certificates conforming to the EPC e-Mandates e-Operating Model Detailed Specifications 3. Subscribers must enroll for certificates issued by approved CAs [5] listed in the TSL. Examples of Subscribers are Routing Services and Validation Services processing SEPA e-Mandates.
- *Relying parties* – all entities that may act in reliance of certificates issued by Certification Authorities and in use by Subscribers. Relying parties may or may not also be Subscribers. Examples of Relying parties are Creditors and Creditor Banks processing SEPA e-Mandates.

1.4 TSL Usage

The TSL may only be used within applications, services and frameworks under regulation of the TSL Promoter. The TSL must not be used in any contexts other than these.

Further detailed restrictions to the TSL usage are defined in section 4.5.

[2] http://www.multicert.com

1.5 Policy Administration

1.5.1 Organization Administering the Document

MULTICERT – Serviços de Certificação Electrónica S.A.
Lagoas Park
Edifício 3, Piso 3
2740-266 Porto Salvo, Oeiras
PORTUGAL

1.5.2 Contact Person

EPC TSL Policy Administration
MULTICERT – Serviços de Certificação Electrónica S.A.
Lagoas Park
Edifício 3, Piso 3
2740-266 Porto Salvo, Oeiras
PORTUGAL

Tel: +351 21 712 3010
Fax: +351 21 712 3011
E-mail: epc-tsl@multicert.com

1.5.3 Organization Determining TSL Suitability for the Policy

Certification Authority Supervisory Board
European Payments Council AISBL
Cours Saint-Michel 30A
B-1040 Brussels
Belgium

Tel: +32 2 733 35 33
Fax: +32 2 736 49 88
E-mail: secretariat@epc-cep.eu

1.5.4 Policy Approval Procedure

The approval procedure of this policy follows the provisions defined in section 9.10.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Acronym	Definition
AR	Audit Report
CA	Certification Authority
CAP	Corrective Action Plan
CC	Common Criteria
DER	Distinguished Encoding Rules

Acronym	Definition
EAL	Evaluation Assurance Level (CC)
eOM	e-Operating Model
EPC	European Payments Council
ETSI	European Telecommunications Standards Institute
FAR	Final Audit Report
FIPS	United State Federal Information Processing Standards
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
PAR	Preliminary Audit Report
PKI	Public Key Infrastructure
RFC	Request For Comments
RSA	Rivest, Shamir, and Adelman (the cryptograhic algorithm)
SHA	Secure Hash Algorithm
TS	Technical Specification (ETSI)
TSL	Trust-service Status List
WG	Working Group
XML	Extensible Markup Language

Table 1 – Acronyms used throughout the TSL Policy

1.6.2 Definitions

Term	Definition
Approval	Assertion that an electronic trust service, falling within the oversight of a particular scheme, has been either positively endorsed (active approval) or has received no explicit restriction since the time at which the scheme was aware of the existence of the said service (passive approval).
Certificate	The public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it.
Certification Authority	An authority trusted by one or more users to create and assign public-key certificates.
Private Key	Key of a user's key pair which is known only by that user
Public Key	Key of a user's key pair which is publicly known.
Public Key Infrastructure	The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.
Scheme	An organized process of supervision, monitoring, approval or such practices that are intended to apply oversight with the objective of ensuring adherence to specific criteria in order to maintain confidence in the services under the scope of the scheme.
Trust-service Status List	Supervision/Accreditation Status List of certification services from Trust Service Providers, which are supervised/accredited by the scheme promoter/operator.
TSL Policy	A statement of the practices that a TSL Scheme Operator employs in issuing TSLs.

Table 2 – Definitions used throughout the TSL Policy

2 Publication and Repository Responsibilities

The TSL Scheme Operator maintains a public web site continuously available where the following information can be obtained:

- the most updated version of this TSL Policy
- the TSL file in XML format
- the DER encoded X.509 certificate used to sign the published TSL
- the SHA-256 hash of the DER encoded X.509 certificate used to sign the published TSL
- the DER encoded X.509 certificates composing the certification path up to a self-signed X.509 CA certificate of the X.509 certificate used to sign the published TSL
- the SHA-256 hash of the DER encoded self-signed X.509 CA certificate included in the certification path of the X.509 certificate used to sign the published TSL

The web site is accessible by HTTP and HTTPS.

3 Identification and Authentication

3.1 Naming

The names referring to any of the organizations, trademarks and services indicated in the TSL are the formal names under which the associated legal entities or mandated organizations are officially registered and are liable for.

The formal names must be unique, i.e., a formal name cannot refer to two or more distinct organizations, trademarks and services.

Where explicitly allowed by the TSL technical standard, additional alternative names can be provided (for example, to refer to the commonly known name on the market).

3.2 Initial Identity Validation

All data submitted by the applicant participants is confirmed by the TSL Promoter and/or the TSL Scheme Operator according to the defined validation processes.

In particular, the existence, correctness and right to use the provided names, addresses and contacts are verified.

As part of the initial identity validation, a trusted channel is established with the applicant for further communications.

3.3 Identification and Authentication for Revocation Requests

Revocation requests – hereby understood as revocation or suspension requests – from CAs are authenticated through the trusted communication channels established at the initial identity validation process (section 3.2).

The TSL Promoter is also granted the right to request revocations to the TSL Scheme Operator through the defined revocation processes.

4 TSL Life-Cycle Operational Requirements

4.1 CA Application

Authorized representatives of a CA may apply to the TSL Promoter for inclusion on the TSL.

The CA representative(s) must provide all requested information by the TSL Promoter according to the established processes. The provided information must be authentic, correct, complete and true.

4.2 CA Application Processing

The TSL Promoter validates the identity of the CA and its representative(s) in accordance with the terms defined in section 3.2. A trusted communication channel is established to exchange the information required to fulfil the acceptance conditions and complete the defined application process.

Should the applicant CA fail any of the acceptance conditions, the TSL Promoter and/or the TSL Scheme Operator are reserved the right to terminate the application process without the right for indemnities or refunds of any type for any fees that may have already been charged.

4.3 TSL Issuance

TSLs are issued in a regular periodic basis by the TSL Scheme Operator.

The TSL Scheme Operator is reserved the right to issue extraordinary TSLs before the next regular scheduled issuance under the following circumstances:

a) a CA revocation or suspension request is accepted

b) a CA fulfilling the conditions to be considered "urgent"

c) other circumstances under the criteria of the TSL Scheme Operator

The TSL Scheme Operator is exempt from explicitly notifying any of the TSL participants about extraordinary TSL issuances. However, TSL participants may subscribe to a web syndication service (RSS) provided by the TSL Scheme Operator which contains notifications about TSL issuances.

The information contained in the issued TSLs corresponds to the provided information by the CA representative(s) and confirmed with the available means by the TSL Promoter and TSL Scheme Operator.

4.4 TSL Acceptance

Each issuance of a TSL is considered accepted if no objections are presented to the TSL Scheme Operator within the lifetime allowed for the TSL usage, as defined in section 4.5.

4.5 TSL Usage

Usage of the TSL is only permitted by a Relying Party if:

a) the present TSL policy is fully accepted and understood

b) the TSL is accepted in accordance with the terms defined in section 4.4

c) the TSL is used during its lifetime (between the *List issue date and time* and the *Next update* TSL fields)

d) the TSL is used according to the technical details defined in the TSL specification ETSI TS 102 231

e) the Relying Party obtains assurance about the validity of the TSL and specifically, but not exclusively, about the:

e.1. TSL digital signature

e.2. TSL lifetime

e.3. TSL signing certificate lifetime

e.4. TSL signing certificate revocation status

e.5. certification path of the TSL signing certificate

e.6. issuance of extraordinary TSLs, for which relying parties shall check periodically at reasonable intervals

The TSL is published according to the terms defined in chapter 2.

4.6 CA Modification

CAs are responsible to communicate to the TSL Scheme Operator through the established trusted channels any relevant modifications to the data submitted during the application process.

4.7 CA Revocation and Suspension

A CA suspension on the TSL shall occur whenever enough evidences (formal or informal) are collected to create reasonable doubts about the integrity of the information or the services provided by the CA or to fail the acceptance conditions at any point in time. The informal evidence-based suspicion shall be communicated by the CA to the TSL Scheme Operator, which then suspends the CA in the TSL.

Following the CA suspension process, further investigations are conducted to either confirm the suspicion and revoke the CA, or to refute the suspicion and reactivate the CA.

A CA revocation on the TSL shall occur whenever enough formal evidences are collected confirming that the integrity of the information or the services provided by the CA have been compromised or to fail the acceptance conditions at any point in time. The investigation results are evaluated by the TSL Promoter.

Whenever a TSL revocation or suspension is processed, a new TSL is issued and published according to the terms defined in section 4.3.

4.8 CA End of Subscription

A CA may end a subscription to be listed on the TSL by not renewing its periodic subscription. The CA will continue to be listed in the TSL with status ”expired”.

5 Management, Operation and Physical Controls

MULTICERT has implemented specific policies and rules specifying the management, operation and physical controls in support of the security requirements described in this policy.

This chapter presents an overview of the adopted security measures that allow the safe operation of the TSL.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

MULTICERT site facilities are designed to provide an environment that allows access control and auditing of critical systems, while being physically protected from unauthorized access, damage or interference.

The conceived architecture uses the concept of *defence in depth* by having multiple increasing levels of security. This ensures that access to the next higher level of security is only possible when the level immediately before has been reached. It is not possible at any place of the facilities to access the security level (n) from other than the level (n-1).

The security policies of the TSL are administered in a secured room located inside another high security zone, and within a building that meets several safety conditions, including controls that detect, deter and prevent unauthorized accesses based on multiple levels of physical security.

The two high security zones are areas that satisfy the following characteristics:

a) walls of masonry, concrete or brick;

b) ceiling and floor with similar construction to the walls;

c) no windows;

d) security fire steel doors featuring electronic security locks, panic bar and steel hinges and jambs hidden from the inferior security level.

Additionally, the following security conditions are guaranteed in the environment:

- clearly defined security perimeters;
- walls, floors and ceilings in brick with no windows that prevent unauthorized access;
- access doors to the safe environment featuring high security bolts and anti-theft locks

- the perimeter of the building is considered to be sealed to the extent that there are no doors, windows or other uncontrolled breaches allowing unauthorized accesses;
- access to the environment must pass through areas of human control along with other control means, thus effectively restricting physical access only to authorized personnel.

5.1.2 Physical Access

MULTICERT systems are protected by a minimum of four physical security hierarchical levels (the building itself (1), a restricted area (2), a security buffer zone (3) and the high security room (4)) ensuring that access to a higher level of security is possible only if the necessary privileges to reach the level immediately above have been granted.

Sensitive operational activities on the system, creation and storage of cryptographic material and other critical activities within the lifecycle of the TSL occur within the more restricted area of high security. Access to each level of security requires the use of a magnetic card authentication. Physical accesses are automatically recorded and stored in a closed circuit TV for audits and logged in a database.

Unescorted personnel, including unauthenticated employees or visitors, are not permitted to enter and stay in the security areas. Unless all staff circulating within these security areas are know to each other, it is compulsory to wear their access card visibly, as well as ensuring that unrecognized individuals have their personal access card visible.

The access to the more restricted area of high security has access controls in place, such that any operation performed inside the secure room is under surveillance of at least two persons. Two factor authentication mechanisms are used, including biometric authentication.

5.1.3 Power and Air Conditioning

The secure environment of MULTICERT has redundant equipment, which ensures proper operational conditions 24 hours a day / 7 days a week. In particular, the following measures are adopted:

- Continuous, uninterrupted electric power supply sufficient to independently maintain the power grid during reasonable periods of power failure and protect the infrastructure equipment against power fluctuations that may cause damage (the equipment consists of redundant uninterruptible power supply batteries and diesel electricity generators), and
- Cooling/ventilation/air conditioning continuously controls the temperature and humidity ensuring adequate conditions for the normal functioning of all electronic equipment and mechanical components present in the environment. A temperature sensor triggers a GSM alert whenever the temperature is outside the normal range. This alert starts automatic GSM phone calls with a previously recorded message to the maintenance team.

5.1.4 Water Exposing

The high security zones are equipped with mechanisms (flood detectors) to minimize the impact of floods.

5.1.5 Fire Prevention and Protection

The secure environment of MULTICERT is equipped with the necessary mechanisms for preventing and extinguishing fires or other incidents arising from fire or smoke. These mechanisms are in accordance with existing regulations and include:

- Fire detection and fire alarm systems deployed at various levels of physical security,
- Both fixed and mobile fire extinguishing equipments are available, placed in strategic locations and easy access so they can be readily used,
- Well defined emergency procedures in case of fire.

5.1.6 Media Storage

All media containing sensitive information including software, production data, auditing information and backups are kept in safes and security cabinets inside the high security zone, as well as in a separate environment outside the building with appropriate physical and logical access controls, described in written procedures, to restrict access only to authorized elements of the Working Groups. Beyond the access restrictions, the external environment has also implemented mechanisms to protect against accidents (eg, caused by water or fire).

Whenever sensitive information is transported from the high security zone to the external environment (for backup purposes, for example), the process runs under the supervision of at least 2 (two) members of the Working Group entitled and responsible to ensure the information transport to the destination. The media containing the information must be under visual inspection of the members of the Working Group at all time.

In situations involving the physical movement of data storage hardware (eg, hard disks) outside the zone of high security, for reasons other than backups, each hardware item is inspected to check if it contains sensitive data. In these situations, the information has to be eliminated by using all necessary means to that end (low-level formatting of the hard drive, zeroize the cryptographic hardware or even physical destruction of the storage equipment).

5.1.7 Waste Disposal

Documents and other paper-based materials containing sensitive information shall be shredded before disposal.

Cryptographic equipment and physical or logical access keys are destroyed following the recommendations of the manufacturer, before disposal. Other storage equipment (e.g. hard disks, tapes) is permanently erased via secure low-level formatting and/or physical destruction.

Retrieval or recovery of any kind of information from the media used to store or transmit sensitive information after its elimination and disposal is not possible.

5.1.8 Off-Site Backup

All backups are kept in a secure environment in external facilities, inside safes and cabinets located in secure areas with physical and logical access controls restricted to authorized personnel.

Protection against accidental damage (eg, caused by water, fire or power surges and outages) is also implemented.

5.2 Procedural Controls

The activity of a TSL Scheme Operator depends on the coordinated and complementary actions of an extensive range of human resources.

In this section, the practices in support of the trust roles and associated responsibilities are described. This section also includes the separation of duties in terms of roles that can not be performed by the same individuals.

5.2.1 Trusted Roles

All personnel (trusted persons) that are granted access to the infrastructure must belong to one of the following trusted roles, designated as Working Groups:

- Policy Working Group;
- Audit Working Group;
- Operation Working Group;
- Authentication Working Group;
- Setup Working Group;
- Management Working Group;
- Custody Working Group.

Trusted persons include, but are not limited to, MULTICERT employees, contractors and consultants. Each of the trusted persons is screened and trained before being admitted and assigned a trusted role, as described throughout section 5.3.

5.2.2 Number of Persons Required per Task

Strict control procedures require the division of responsibilities based on the specifics of each Working Group, and to ensure that sensitive tasks can only be performed by a multiple set of people certified.

Operations inside the secure room must be performed by a minimum of 2 (two) persons, one of them being a system auditor.

Whenever sensitive information is transported from the high security zone to the external environment (for backup purposes, for example), the process runs under the supervision of at least 2 (two) members of the Working Group entitled and responsible to ensure the information transport to the destination.

5.2.3 Human Resources

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations.

MULTICERT has established that Trusted roles are grouped into seven different categories (named as working groups), to ensure that multiple Trusted Persons are required to perform sensitive tasks.

5.2.3.1 Policy Working Group

The purpose of this group is to define the TSL policies and guarantee they are appropriate, updated and available to the selected target audiences. This group must have a minimum of two members.

The group duties are:

- to define the TSL policies,
- to guarantee that the policies are appropriate, updated and available to the selected target audiences.

The Policy Working Group plays part of the "Security Officer" role, as defined in CWA 14167-1 [10].

5.2.3.2 Audit Working Group

This group audits the execution of TSL processes and ceremonies, registering sensible operations and validating the security of all resources used. This group must have a minimum of two members and at least one must be present in all operations performed in the high security room.

The group duties are:

- to sanction the exactness of processes,
- to investigate suspicions of procedural fraud,
- to check functionality of existing safety controls (alarm devices, fire detectors, etc)
- to register all security auditable procedures,

- to register all security auditable checks.

The Audit Working Group plays the "System Auditor" role, as defined in CWA 14167-1 [10].

5.2.3.3 Operation Working Group

This group is responsible for the routine tasks of the TSL everyday operation, including backup operations and monitoring hardware and software malfunctions. The members of this group must be divided in at least 2 (two) subgroups (named "Subgroup 1" and "Subgroup 2"), composed of (at least) 2 (two) members each. The membership of one subgroup is exclusive, meaning that one group member can only belong to one of the subgroups.

The group duties are:

- to perform TSL routine operations,
- to perform system backups,
- to perform system monitoring,
- to monitor, report and quantify hardware and software incidents and malfunctions.

The Operation Working Group plays the "System Administrator", "System Operator" and "Registration Officer" roles, as defined in CWA 14167-1 [10].

5.2.3.4 Authentication Working Group

This group is responsible for providing, managing and keeping, all non personal passwords and authentication tokens. This group must also take adequate measures in case of a security token or password compromise. The members of this group must be divided in at least 2 (two) subgroups (named "Subgroup 1" and "Subgroup 2"), composed of (at least) 2 (two) members each. The membership of one subgroup is exclusive, meaning that one group member can only belong to one of the subgroups.

No member of this group is allowed to enter the secure room without the presence of a member of the Operation Working Group and/or Auditing Working Group.

The group duties are:

- to manage all non personal passwords,
- to maintain an inventory of all existing authentication tokens and, when these tokens are entrusted to someone, to register the identification of the member(s) in its possession,
- to maintain an inventory of all passwords used in the system and, when these passwords are entrusted to someone, to register the identification of the member(s) in their possession,
- to entrust each of the group members with no more than the needed artefacts to perform his/her duties,

- to register the return of artefacts used in ceremonies,
- to register the change of authentication passwords used by the system,
- to register the loss of an artefact used by the system,
- to register the compromise of an artefact used by the system,
- to evaluate business risks concerning the loss or compromise of an artefact,
- to take active measures to prevent the compromise of the system in case of an artefact loss or compromise,
- to evaluate requests for documentation replication.

The Authentication Working Group fulfils the part of the "Security Officer" role, as defined in CWA 14167-1 [10].

5.2.3.5 Setup Working Group

This group is responsible for the initial setup of the TSL (hardware, software, passwords), until its initialization. This group must have a minimum of one member.

The group duties are:

- to install and configure the TSL base software,
- to setup, install and configure the TSL hardware,
- to setup any passwords, for the first time, that will have to be changed afterwards by the appropriate group.

5.2.3.6 Management Working Group

This group is responsible for appointing the working group's members, as well as approving documents. This group must have a minimum of two members.

The group duties are:

- to manage the "Management Environment",
- to revise and approve documentation supporting the TSL activity,
- to appoint members of the working groups,
- to publish identification of all individuals that are part of working groups, in one or more locations, that can be easily accessed by authorized parties.

5.2.3.7 Custody Working Group

This group is responsible for safekeeping sensitive items (authentication tokens, etc) in their facilities. This group must use the secure environments made available to them in order to keep items in their possession.

The group duties are:

- to guard sensitive items, such as authentication tokens, etc, using adequate means to accomplish the security requirements,
- to safely deliver items to authorized group members that are explicitly allowed to access them, after following the proper entrust procedures.

5.2.4 Number of persons required per task

MULTICERT enforces rigorous control procedures to ensure the segregation of duties based on working group membership and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The internal control procedures are designed to ensure that at a minimum, two trusted persons are required to have either physical or logical access to security devices. Access to TSL cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold separate parts of the activation key and vice versa.

5.2.5 Roles Requiring Separation of Duties

The following table defines the membership incompatibilities (indicated by ✖) between a group relative to the other groups.

		Setup	Policy	Operation		Authentication		Audit	Custody	Management
				Subgroup 1	Subgroup 2	Subgroup 1	Subgroup 2			
Setup								✖	✖	✖
Policy								✖	✖	✖
Operation	**Subgroup 1**				✖	✖	✖	✖	✖	✖
	Subgrup 2			✖		✖	✖	✖	✖	✖
Authentication	**Subgroup 1**			✖	✖		✖	✖	✖	✖
	Subgroup 2			✖	✖	✖		✖	✖	✖
Audit		✖	✖	✖	✖	✖	✖		✖	✖
Custody		✖	✖	✖	✖	✖	✖	✖		✖
Management		✖	✖	✖	✖	✖	✖	✖	✖	

5.3 Personnel Security Controls

The engagement of staff in the Working Groups is subject to all of the following conditions:

- Be formally nominated for the position;
- Have received adequate training;
- To prove his identity by using reliable and updated documentation issued by a trustful source;
- Provide proof of not having a criminal record;
- Provide proof of possessing the qualifications and experience required;
- Formally commit to not to disclose without explicit permission from the legal representatives of the TSL Scheme Operator any information about the TSL service, its operation, environment and human resources;

- Formally commit to perform the functions for which he was appointed and not assume responsibilities that may raise ethical issues. Thus, it is necessary to declare not only explicit knowledge of the terms and conditions of the job, but also the ability and willingness to do it.

5.3.1 Qualifications, Experience, and Clearance Requirements

The admission of new members in the Working Groups is limited to the presentation of knowledge, skills and experience evidences necessary to perform the tasks of the Working Groups. Additionally, governmental clearances of at least equivalent to NATIONAL SECRET are required.

5.3.2 Background Check Procedures

A background check is part of the process of accreditation of individuals appointed to hold positions in any of the trusted roles. The background check includes but is not limited to:

- Confirmation of identification documents issued by trustful sources, and
- Investigation of criminal records.

5.3.3 Training Requirements

Appropriate training is provided to all members of the Working Groups in order to execute their tasks satisfactorily and competently.

The elements of the Working Groups are subject to a training plan, covering the following topics:

a) digital certificates, Public Key Infrastructure and TSL;

b) information security awareness;

c) specific training for their role within the Working Group;

d) operating software and / or hardware used by the TSL infrastructure;

e) TSL Policy;

f) disaster recovery;

g) procedures for business continuity; and

h) basic legal issues concerning the provision of trust services.

5.3.4 Retraining Frequency and Requirements

Whenever considered necessary, additional training is provided to the Working Group members in order to ensure that they execute their tasks satisfactorily and competently. In particular, retraining is provided, but not limited to, the following events:

- a technological change, introduction of new tools or modification of procedures,

- the TSL Policy is changed.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

It is considered as unauthorized actions all actions that violate the TSL Policy, whether made intentionally or caused by negligence.

Sanctions are applied to all individuals who undertake unauthorized actions or making unauthorized use of systems in accordance with the applicable work rules, national laws and national security laws.

5.3.7 Independent Contractor Requirements

Consultants or independent service providers are allowed access to the high-security zones provided that they are always accompanied and directly supervised by members of the Working Groups.

The procedures for background checks to be applied in these situations are the same as those listed in section 5.3.2.

5.3.8 Documentation Supplied to Personnel

Members of the Working Groups are provided with all appropriate information to enable them to perform their duties competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Significant events generate auditable records. As a minimum, these include the following:

- CA requests (such as initial application, suspension request,...)
- CA application conformance testing
- TSL issuance
- TSL publication;
- Security related events, including but not limited to:
    - the attempts to access (with or without success) to sensitive resources of the TSL infrastructure;
    - the operations carried out by members of the Working Groups,

- entry / exit of the several physical security zones.

The entries in the records include the following information:

- Serial number of the event;
- Date and time of the event;
- Identity of the subject that caused the event;
- Category of the event;
- Description of the event.

5.4.2 Frequency of Processing Log

Records are analysed and reviewed on a regular basis, and additionally whenever suspicious or abnormal activities or threats of any kind occur. Actions taken based on information from the records are documented.

5.4.3 Retention Period for Audit Log

The records are kept available for at least 2 (two) months after processing, and then archived on the terms described in section 5.5.

5.4.4 Protection of Audit Log

The records are reviewed only by authorized members of the Working Groups.

The records are protected by auditable electronic mechanisms to detect and prevent the occurrence of tampering, removal, or other forms of unauthorized manipulation of data.

5.4.5 Audit Log Backup Procedures

Regular backups of the records are created and stored into high-capacity storage systems.

5.4.6 Audit Collection System (Internal vs. External)

The records are collected simultaneously inside and outside the TSL system.

5.4.7 Notification to Event-Causing Subject

Auditable events are recorded in the audit system and stored safely, without necessarily notifying the subject that caused the event.

5.4.8 Vulnerability Assessments

Auditable records are regularly reviewed to minimize and eliminate any potential attempts to breach the system security.

5.5 Records Archival

5.5.1 Types of Records Archived

All auditable data indicated in section 5.4.1 is archived.

5.5.2 Retention Period for Archive

Archives are retained for a period not less than 10 (ten) years.

5.5.3 Protection of Archive

Archives are protected in such a way that:

- Only authorized members of the Working Groups may consult and have access to the files,
- The files are protected against any attempt to modification or removal,
- The files are protected against deterioration of the media where they are stored, through periodic migration to new media,
- The files are protected against obsolescence of hardware, operating systems and other software, by having the hardware, operating systems and other software become part of the archive itself, allowing access and use of stored records at any point in time in the future, and
- File copies are safely stored in secure external sites.

5.5.4 Archive Backup Procedures

Backup copies of files are performed incrementally or in total and stored in appropriate long term storage devices.

5.5.5 Requirements for Time-Stamping of Records

Some file entries may contain information on date and time. Such date and time information is based on a trusted time source.

5.5.6 Archive Collection System (Internal or External)

The archive data collection systems are internal to the TSL infrastructure.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to the archive information is limited to authorized members of the Working Groups. The file integrity shall be checked at inspection or restoring of the archive.

5.6 Key Changeover

TSL signing key pairs are disabled whenever their maximum allowed lifetime is reached. The disabled key pairs are replaced in advance with new key pairs earlier that the maximum lifetime in order to allow a smooth transition from the old key pair to the new one.

5.7 Compromise and Disaster Recovery

This section describes the requirements related to notification and recovery procedures in case of a disaster or security compromise.

5.7.1 Incident and Compromise Handling Procedures

Backups of archived records are stored in safe external environments which are available in case of disaster or compromise.

A key changeover as defined in section 5.6 may be executed in the event of a disaster or compromise.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the case of computing resources, software and/or data being corrupted or is suspected of corruption, the backup copies of the archived records can be obtained to verify the integrity of the original data.

If confirmed that the computing resources, software and / or data are corrupted appropriate actions shall be taken to respond to the incident. The response to the incident may include:

- the reestablishment of the equipment / corrupted data,
- using similar equipment, and / or
- recovering backups and archived records.

Until the regular safe operating conditions are restored and re-established, the TSL Scheme Operator will suspend its services and shall notify the TSL Promoter and the CAs.

5.7.3 Private Key Compromise Procedures

In the event of a TSL signing private key compromise to be committed or suspected, appropriate actions shall be taken in response to the incident. The answers to this incident may include:

- Request revocation of the TSL signing certificate,
- Notification of the TSL Promoter and all active CAs,
- TSL signing key pair changeover as described in section 5.6.

5.7.4 Business Continuity Capabilities after a Disaster

MULTICERT has the necessary computing resources, software, backups and records stored on its secondary security site facilities to re-establish or restore essential operations (issuing and publication of TSLs) after a disaster occurrence.

5.8 TSL Termination

In case of cessation of activity as a service provider, MULTICERT shall, with at least three months in advance, proceed with the following actions:

a) inform all active CAs;

b) request revocation of the TSL signing certificate;

c) carry out a final notification to CAs 2 (two) days before the formal cessation of the activity;

d) ensure the transfer (for retention by another organization) of all information on the activities of the TSL, including any cryptographic material, scripts, documentation files (internal or external) repositories, event log archives and backups.

In case of changes in the body/organization responsible for managing the activity of the TSL, it must inform the entities listed in the above paragraphs.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The generation of cryptographic keys for the TSL signing certificate is performed exclusively by members of the Authentication Officers Working Group under continuous supervision of a System Auditor. The ceremony is planned and audited in accordance with written procedures describing the operations to be performed. All key generation ceremonies are logged, dated and signed by the elements involved in the Working Group.

The cryptographic hardware used for key pair management of the TSL signing certificate, including generation, storage and usage, is compliant with FIPS 140-2 level 3 and/or Common Criteria EAL 4+. Key access is protected by security policies and division of responsibilities between the Working Groups.

6.1.2 Key Sizes

Key pairs must be of sufficient length to prevent possible attacks from cryptanalysis to discover the private key corresponding to the key pair in its period of use. The following are the minimum key lengths:

- 4096 bit RSA key pairs for Certification Authorities included in the certification path of the TSL Signing Certificate
- 2048 bit RSA key pairs for the TSL Signing Certificate

6.2 Private Key Protection and Cryptographic Module Engineering Controls

This section describes the requirements for private key protection and cryptographic modules in use on the TSL. MULTICERT has implemented a combination of physical, software and procedural controls, to ensure confidentiality and integrity of the TSL private keys.

6.2.1 Cryptographic Module Standards and Controls

For private key generation and storage of the TSL signing certificate, MULTICERT uses hardware cryptographic modules certified at FIPS 140-2 Level 3 and/or Common Criteria EAL 4+.

6.2.2 Private Key (m out of n) Multi-Person Control

The activation data for the TSL signing private key held in the cryptographic module is split into multiple secret shares that are of exclusive individual knowledge of each of the responsible WG members.

6.2.3 Private Key Escrow

TSL signing certificate private keys are not escrowed.

6.2.4 Private Key Backup

Backup copies are not performed for the TSL signing certificate key pairs. In the event of a data loss, a new key pair is generated and the TSL signing certificate is replaced in the same operational and security conditions as the previous one.

6.2.5 Private Key Archival

Upon expiration or renewal of the TSL signing certificate, the corresponding private key is not archived or retained in any form.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The private key of the TSL signing certificate shall never be transferred from the original cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

The private key of the TSL signing certificate held in the cryptographic module is stored in encrypted form.

6.2.8 Method of Activating Private Key

The activation data of the TSL signing certificate private key held in the cryptographic module is protected as described in section 6.2.2. Its activation requires two secret shares, thus providing a dual control protection mechanism.

The private key is active until a deactivation occurs as described in section 6.2.9.

6.2.9 Method of Deactivating Private Key

The private key of the TSL signing certificate held in the cryptographic module is deactivated upon removal of the token reader or system shutdown.

Once the key has been deactivated, it remains inactive until re-activation occurs, as described in section 6.2.8.

6.2.10 Method of Destroying Private Key

Private keys are destroyed in accordance with manufacturer guidelines, which may include key overwriting, token zeroization or token destruction.

This operation must be performed locally in the high security room and is limited to authorized personnel.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys of CA services are part of the registration entries and are included in the TSL file. MULTICERT performs regular backups of such information.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The usage period of the private TSL key is determined by the TSL signing certificate, such that after certificate expiration the keys can no longer be used, resulting in the permanent cessation of its operation and the intended usage.

The TSL signing certificate validity is 5 (five) years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data is generated at cryptographic module initialization by the authorized personnel. Afterwards, it is entered into the system service configuration artefacts.

6.4.2 Activation Data Protection

The activation data is recorded and stored in a vault with limited access to authorized personnel.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

Should the activation data need to be transmitted, it shall be protected against information loss, theft, modification of data and unauthorized disclosure.

6.4.3.2 Activation Data Destruction

The activation data is destroyed by means of physical destruction when the corresponding cryptographic module is decommissioned or destroyed.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Access to the TSL servers is restricted to members of the Working Groups which have been granted such privileges. The TSL service is a continuous online service, with no direct inbound or outbound Internet traffic. All operations to be performed by members of the TSL Scheme Operator working groups are executed inside the high security room, under surveillance of at least two authorized members.

The TSL service has border protection devices, including firewall systems, as well as sufficient and appropriate mechanisms in order to meet requirements for identification, authentication, access control, administration, auditing, reuse, accountability and recovery services and information exchange.

6.5.2 Computer Security Rating

The various products and systems employed by MULTICERT are reliable and protected against modifications.

The cryptographic module hardware meets the standard Common Criteria EAL 4 + and/or FIPS 140-2 level 3.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The applications developed and implemented by MULTICERT are in accordance with MULTICERT rules of system development and change management.

The applications provided by third parties are developed and implemented in accordance with their rules of system development and change management.

MULTICERT provides an auditable methodology for verifying that the software has not been changed prior to its first use. All configuration and software changes are implemented and logged and audited by members of the Working Groups.

6.6.2 Security Management Controls

MULTICERT has mechanisms and/or Working Groups dedicated to the control and monitoring of the TSL systems.

MULTICERT performs regular checks to the integrity of the installed software as well as at its first use.

6.6.3 Life Cycle Security Controls

The update and maintenance operations of TSL products and systems follow the same controls as the original equipment and are executed by members of the Working Groups with appropriate training to do so by following the procedures established for that purpose.

6.7 Network Security Controls

The TSL infrastructure is provided with border protection devices, including firewall systems, as well as sufficient and appropriate mechanisms in order to meet requirements for identification, authentication, access control, administration, auditing, reuse, accountability and recovery services and information exchange.

6.8 Time-stamping

TSL files and other registration data entries contain date and time information, which is synchronized with a trusted network time source cluster and checked periodically.

7 Profiles

7.1 TSL Profile

The following table defines the properties and values for each field in the TSL. The TSL structure presented is according to version 3.1.2 of ETSI TS 102 231, and the defined values follow the Detailed Specifications for TSLs for EPC Approved Certification Authorities (CAs) in support of SEPA e Mandate Services (EPC249-09). [4]

Field	Mandatory	Value	Comment
Information on TSL Issuing Scheme			
TSL Tag	Required	`http://uri.etsi.org/02231/TSLTag`	
TSL Version Identifier	Required	`3`	corresponding to ETSI TS 102 231 version 3.1.2
TSL Sequence Number	Required	`1`	incremented by `1` at each subsequent release of the TSL
TSL Type	Required	`http://uri.etsi.org/TrstSvc/TSLtype/generic/EPC-ApprovedList`	
Scheme Operator Name	Required	`MULTICERT - Serviços de Certificação Electrónica S.A.`	formal legal name of the TSL Scheme Operator
Scheme Operator Address	Required	**Street Address:** `Lagoas Park, Edificio 3, Piso 3` **Locality:** `Porto Salvo, Oeiras` **Postal Code:** `2740-266 PORTO SALVO` **Country Name:** `Portugal` **Scheme Operator Email Address:** `epc-tsl@multicert.com`	address of the TSL Scheme Operator
Scheme Name	Required	`EPC Approved CA Services`	
Scheme Information URI	Required	`http://www.europeanpaymentscouncil.eu/content.cfm?page=trust_service_status_list`	URI where users and relying parties can obtain information about the TSL

Field	Mandatory	Value	Comment
Status Determination Approach	Required	http://uri.etsi.org/TrstSvc/TSLType/StatusDetn/active	
TSL Policy/Legal Notice	Required	http://pki.multicert.com/epc-tsl/MULTICERT_PJ.EPC_24_0001_en.pdf	URL where this TSL policy can be downloaded
Historical Information Period	Required	3653	value in days, corresponding to ten years
List Issue Date and Time	Required	AAAA-MM-ddTHH:MM:ssZ	
Next Update	Required	AAAA-MM-ddTHH:MM:ssZ	No longer than **List Issue Date and Time + 7 days**
Distribution Point	Required	http://pki.multicert.com/epc-tsl /multicert-epc-eom-tsl.xml	
List of Trust Service Providers	Optional		Field **absent if** no CA services are or have been approved.
TSP Information			
TSP Name	Required		legal entity responsible for the CA services that are or were approved under this scheme
TSP Trade Name	Optional		alternative name under which the CA identifies itself in the specific context of the provision of its services that are to be found in the TSL
TSP Address	Required	**Street Address:** **Locality:** **Postal Code:** **Country Name:** **Scheme Operator Email Address:**	address of the CA holder company

Field	Mandatory	Value	Comment
TSP Information URI	Required		URI(s) where users (e.g., relying parties) can obtain CA-specific information
List of Services	Required		contains a sequence of the approved CA services and respective approval status
Service Information			
Service Type Identifier	Required	`http://uri.etsi.org/TrstSvc/Svctype/CA/PKC`	Certification Authority issuing publickey certificates
Service Name	Required		name under which the CA services are provided
Service Digital Identity	Required		relevant X.509v3 certificate being a representation of the public key(s) that the CA uses for providing the service

Field	Mandatory	Value	Comment
Service Current Status	Required	Choose one of the following: • `http://uri.etsi.org/TrstSvc/Svcstatus/inaccord` • `http://uri.etsi.org/TrstSvc/Svcstatus/expired` • `http://uri.etsi.org/TrstSvc/Svcstatus/suspended` • `http://uri.etsi.org/TrstSvc/Svcstatus/revoked`	• *Accordance*: the service is approved according to the dedicated approval process • *Expired*: the service is no longer approved, e.g. due to non-renewal or withdrawal by the CA, or cessation of the service • *Suspended*: the service's status is temporarily uncertain whilst checks are made by the TSL Promoter (typically e.g. while a revocation request is being investigated or if action is required to resolve a deficiency in the service fulfilling the scheme approval criteria • *Revoked*: the service has been revoked because it is no longer in accordance with the approval scheme
Current Status Starting Date and Time	Required	`AAAA-MM-ddTHH:MM:ssZ`	the date and time on which the current approval status became effective
Service Supply Points	Required		URI(s) where relying parties can access the service
TSP Service Definition URI	Required		URI(s) where relying parties can obtain service-specific information provided by the CA

Field	Mandatory	Value	Comment
Service Approval History	Required		Field empty if the service has no history prior to the current status. For each change in **Service Information / Service Current Status** that occurred within the **Information on TSL Issuing Scheme / Historical Information Period**, information on the previous approval status shall be provided in descending order of status change date and time
Service Approval History			
Service Type Identifier	Required	`http://uri.etsi.org/TrstSvc/Svctype/CA/PKC`	Value used in **Service Information / Service Type Identifier** when this field represented the current status
Service Name	Required		Value used in **Service Information / Service Name** when this field represented the current status
Service Digital Identity	Required		Value used in **Service Information / Service Digital Identity** when this field represented the current status
Service Previous Status	Required	Choose one of the following: • `http://uri.etsi.org/TrstSvc/Svcstatus/inaccord` • `http://uri.etsi.org/TrstSvc/Svcstatus/expired` • `http://uri.etsi.org/TrstSvc/Svcstatus/suspended` • `http://uri.etsi.org/TrstSvc/Svcstatus/revoked`	Value used in **Service Information / Service Current Status** when this field represented the current status

Field	Mandatory	Value	Comment
Previous Status Starting Date and Time	Required	AAAA-MM-ddTHH:MM:ssZ	Date and time on which the previous status in question became effective, with the format and meaning used in **Service Information / Service Current Status Starting Date and Time**
Signature			
Signed TSL	Required		Added by XMLDSig
Scheme Identification	Required		Added by XMLDSig
Signature Algorithm Identifier	Required		Added by XMLDSig
Signature Value	Required		Added by XMLDSig

Table 3 - TSL Profile

When applicable, the language chosen by default shall be EN.

7.2 TSL Signing Certificate Profile

The following table describes the TSL Signing Certificate profile.

Certificate Component	Section in RFC 5280	Value	Field Type	Comments
Version	4.1.2.1	3	m	
Serial Number	4.1.2.2	*assigned by the CA*	m	

Signature	4.1.2.3	1.2.840.113549.1.1.11	m	value MUST match the OID in signatureAlgorithm (below)
Issuer	4.1.2.4		m	
Country (C)		PT		PrintableString ASN.1 encoding
Organization (O)		MULTICERT - Serviços de Certificação Electrónica S.A.		UTF8String ASN.1 encoding
Organization Unit (OU)		Entidade de Certificação Credenciada		UTF8String ASN.1 encoding
Common Name (CN)		MULTICERT - Entidade de Certificação 001		UTF8String ASN.1 encoding
Validity	4.1.2.5		m	UTC time until 2049, from then on using GeneralisedTime
Not Before		*issuing date*		
Not After		*issuing date* + *1900 days*		approximately five years and two months.
Subject	4.1.2.6		m	
Country (C)		PT		PrintableString ASN.1 encoding
Organization (O)		MULTICERT - Serviços de Certificação Electrónica S.A.		UTF8String ASN.1 encoding
Organization Unit (OU)		TSL Services		UTF8String ASN.1 encoding
Serial Number (SN)		*3-digit sequence number starting in 001*		PrintableString ASN.1 encoding
Common Name (CN)		EPC e-Mandates e-Operating Model TSL Service		UTF8String ASN.1 encoding
Subject Public Key Info	4.1.2.7		m	holds the public key and identify the algorithm with which the key is used (e.g., RSA)

algorithm		1.2.840.113549.1.1.1		corresponds to rsaEncryption. The parameters field MUST have ASN.1 type NULL for this algorithm identifier.
subjectPublicKey		*RSA key with modulus n of 2048 bits*		
X.509v3 Extensions	4.1.2.9		m	
Authority Key Identifier	4.2.1.1		m	
keyIdentifier		7f 33 72 7f 4c da 34 c8 0e a7 75 cb 2e 83 98 1b 06 b8 a6 90	m	same as the subject key identifier value of the issuer's certificate
Subject Key Identifier	4.2.1.2		m	160-bit SHA-1 hash of the subject public key BIT STRING value (excluding tag, length, and number of unused bits)
Key Usage	4.2.1.3		mc	this extension is marked CRITICAL
Digital Signature		1		
Non Repudiation		0		
Key Encipherment		0		
Data Encipherment		0		
Key Agreement		0		
Key Certificate Signature		0		
CRL Signature		0		
Encipher Only		0		
Decipher Only		0		
Certificate Policies	4.2.1.4		m	

policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	m	MULTICERT CA Certificate Practice Statement
policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.multicert.com/pol/cps/MULTICERT_CA.html	m	CPS Pointer Qualifier
policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.7	m	TSL Signing Certificate Policy OID
policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: Certificate issued in accordance with the Certificate Policy in http://pki.multicert.com/pol/cp/tsl.htm	m	the user notice is recommended to be displayed to a relying party when the certificate is used.
Basic Constraints	4.2.1.10		c	this extension is marked CRITICAL
CA		FALSE		
Extended Key Usage	4.2.1.12		m	
keyPurposeID		0.4.0.2231.3.0		id-tsl-kp-tslSigning,, as in ETSI TS 102 231.
CRLDistributionPoints	4.2.1.13		m	
distributionPoint		http://pki.multicert.comt/crl/crl001.crl		
Freshest CRL	4.2.1.15		m	
distributionPoint		http://pki.multicert.comt/crl/crl001_delta.crl		
Internet Certificate Extensions				
Authority Information Access	4.2.2.1		m	
accessMethod		1.3.6.1.5.5.7.48.1	m	Online Certificate Status Protocol (OCSP)
accessLocation		http://ocsp.multicert.com/ocsp	m	

Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	corresponds to sha-256WithRSAEncryption
Signature Value	4.1.1.3	*digital signature issued by the CA*	m	by imprinting this signature, the CA certifies the binding between the public key material and the subject of the certificate.

Table 4 - TSL Signing Certificate Profile

8 Compliance Audit and Other Assessment

Examination of compliance to this Policy and other applicable rules, procedures and processes are performed by the Audit WG members on a regular basis.

Furthermore, the TSL activities are subject to compliance audits conducted by independent third-parties to assess the compliance of the TSL with the requirements of the EPC and the provisions of the underlying exclusive services grant agreement.

8.1 Frequency or Circumstances of Assessment

Compliance audits are conducted on an annual basis. The resulting audit reports are submitted to the TSL Promoter.

8.2 Identity/Qualifications of Assessor

Compliance audits or other assessments are performed by personnel with:

- required qualifications including recognized competency, experience and qualifications proven in the information security area;
- know-how in public key infrastructure technology, information security tools and techniques,
- security auditing certification by a known certification body.

8.3 Assessor's Relationship to Assessed Entity

Compliance audits or other assessments are performed by public firms or personnel independent of MULTICERT.

8.4 Topics Covered by Assessment

The scope of audits and other assessments include compliance with applicable legislation, this Policy and other rules, procedures and processes (especially those relating to key management operations, resources and security controls) supporting the TSL activity.

8.5 Actions Taken as a Result of Deficiency

For all deficiencies resulting from an audit, the auditing process shall proceeds as follows:

a) the auditor documents all deficiencies found during the audit;

b) at the end of the audit, the auditor meets with officials of the TSL Scheme Operator and outlines a Preliminary Audit Report (PAR);

c) the auditor prepares the audit report. This report shall be organized so that all deficiencies are graded and sorted in descending order of seriousness or severity;

d) the auditor submits the Audit Report (AR) to the TSL Promoter for evaluation;

e) after evaluation of the AR by the TSL Promoter, a copy of the Final Audit Report (FAR) is sent to the TSL Scheme Operator;

f) taking into account the deficiencies described in the FAR, the TSL Scheme Operator shall send a Corrective Action Plan (CAP) within 30 (thirty) days to the TSL Promoter, describing reasonable actions, methodologies and timings required to correct the deficiencies;

g) the TSL Promoter evaluates the CAP, and takes one of the following actions:

g.1. accepts the provisions of the CAP, allowing the TSL Scheme Operator to continue operating the TSL until the next regular audit; or

g.2. accepts the provisions of the CAP, allowing the TSL Scheme Operator to continue a conditional operation subject to an extraordinary audit to assess the implementation of the CAP; or

g.3. revokes the TSL activity.

8.6 Communication of Results

The deliverable results identified in section 8.5 shall be reported within the schedule established in the following table:

Deliverable	Auditor	TSL Promoter	TSL Scheme Operator
PAR	end of audit		
AR	15 days after PAR		
FAR		15 days after AR	
CAP			30 days after FAR
CAP evaluation		15 days after CAP	

Table 5 – Audit results communication schedule

9 Other Business and Legal Matters

This section covers general business and legal matters.

9.1 Fees

9.1.1 CA Registration Fee

MULTICERT is entitled to charge fees to the CA for its registration into the TSL.

9.1.2 CA Maintenance Fee

MULTICERT is entitled to charge fees to the CA for its maintenance in the TSL. Should the CA fail to pay the due fees, MULTICERT is entitled to revoke the CA in the TSL.

The service level is monthly evaluated and reported to the CA and the EPC and maintenance credits may apply according to the refund policy (section 9.1.7).

9.1.3 Suspension, Revocation and Re-Activation Fees

Suspensions, revocations and re-activations of CAs are processed free of charge.

9.1.4 TSL Issuance Fee

Issuing TSLs periodically or extraordinarily is free of charge. Nevertheless, MULTICERT is entitled to include an additional fee in the CA Registration Fee (section 9.1.1) for CA explicit requests for immediate TSL issuance after the registration process is successfully concluded.

9.1.5 TSL Access Fee

Access and download of the TSL file hosted in the repository is free of charge.

9.1.6 Fees for Other Services

MULTICERT does not charge a fee for access to this Policy. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with MULTICERT.

9.1.7 Refund Policy

The refund policy is in accordance with the terms of agreement established between the TSL Scheme Operator and the CA.

9.2 Financial Responsibility

The financial responsibility is limited to the terms of agreement established between the TSL Scheme Operator and the CA.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered to be confidential and shall not be disclosed to third parties:

a) the private keys of the TSL signing certificate;

b) all keywords, PINs and other security features relating to the TSL infrastructure;

The following additional information is considered to be confidential and shall not be disclosed to third parties, except for the TSL Promoter and external auditors acting under the provisions of chapter 8:

a) all information relating to safety and control parameters, and audit procedures;

b) identification of members of the Working Groups;

c) any information provided to the TSL Scheme Operator by CAs during the TSL life-cycle, unless explicit authorization for their disclosure has been declared and/or if it is not included in the contents of the TSL;

d) business continuity and recovery plans;

e) transaction records, including complete records and audit logs;

f) all documents supporting the TSL activity, including organizational concepts and financial/trade details. These documents are exclusively handled by members of the Working Groups and subject to restrictions of not being used or disclosed in any way beyond the scope of their duties without prior explicit consent of MULTICERT;

g) the location of the TSL environments and their contents.

9.3.2 Information Not Within the Scope of Confidential Information

The following information is granted public access:

a) TSL files,

b) TSL signing certificates and corresponding certification paths,

c) TSL Policy, and

d) all information classified as "public" (information not expressly considered "public" shall be considered confidential).

The TSL Scheme Operator allows access to non-confidential information while maintaining appropriate security controls to protect its authenticity and integrity.

9.3.3 Responsibility to Protect Confidential Information

Members of the Working Groups or other entities that receive confidential information are responsible for ensuring that it is not copied, reproduced, stored, translated or transmitted to third parties by any means without first having the written consent of MULTICERT.

9.4 Intellectual Property Rights

All intellectual property rights owned by the TSL Scheme Operator, including those relating to information in the certificates, issued TSL files, TSL Policy and any other documents in support of the TSL activity, belong to MULTICERT.

The legitimate holder always retains the right to the brand, product or trade name contained in the TSL.

9.5 Representations and Warranties

9.5.1 TSL Scheme Operator Representations and Warranties

MULTICERT is required to:

a) conduct its operations in accordance with this Policy,

b) state clearly all its public domain TSL Practices in an appropriate document,

c) protect the private keys,

d) issue the TSL in accordance with ETSI TS 102 231 version 3.1.2,

e) issue the TSL in conformance to the information known at the time of its issuance and free os any data entry errors,

f) ensure the confidentiality of the TSL signature creation data

g) use trustworthy systems and products that are protected against unauthorized changes and ensure the technical and cryptographic security of the TSL management and operational processes,

h) use trustworthy systems to store TSL registration data that allow verification of the authenticity and prevent unauthorized persons from changing the data,

i) store issued TSLs unchanged,

j) ensure that it is possible to accurately determine the date and time when a TSL was issued

k) ensure that it is possible to accurately determine the date and time when a CA and its services were activated, suspended or revoked,

l) employ staff with skills, knowledge and experience required to provide TSL services,

m) suspend or revoke a CA according to the terms defined in section 4.7,

n) publish the most updated version of the TSL Policy in the repository and providing access to previous versions at request,

o) timely notify CAs by registered mail and e-mail in copy in case of suspension or revocation of the TSL signing certificate, indicating the underlying motive of this action,

p) cooperate with the audits,

q) operate in accordance with applicable law,

r) protect the cryptographic keys that are under its custody,

s) ensure the availability of the TSL file in the repository,

t) in case of ceasing activity, MULTICERT shall proceed in accordance with the terms defined in section 5.8, and

u) retain all information and documentation relating to a CA and the TSL Policies in effect at any time and for ten years from the time of issue.

9.5.2 Certification Authority Representations and Warranties

It is the obligation of CAs to:

a) submit to the TSL Promoter and TSL Scheme Operator information deemed accurate and complete with respect to data for which they are requested to complete the registration process,

b) inform the TSL Promoter and TSL Scheme Operator of any change to the information provided in the registration process,

c) take all precautions and measures necessary to secure the services provided that are registered in the TSL,

d) request the immediate suspension/revocation if a security compromise is known or suspected to affect in any way the services provided that are registered in the TSL,

e) comply at all time with the acceptance conditions presented at the registration process and additional conditions that may be deemed necessary by the TSL Promoter or TSL Scheme Operator in the future,

f) not monitor, manipulate or reverse engineer the techniques in support of the TSL services, without the prior permission in writing of MULTICERT, and

g) enforce its subscribers to comply with adequate terms of usage of the services provided that are registered in the TSL.

9.5.3 Subscriber Representations and Warranties

It is the obligation of Subscribers to match and limit the use of certificates in accordance with the uses set out in the certificate policies of the issuing CAs.

9.5.4 Relying Party Representations and Warranties

It is the obligation of Relying Parties to:

a) limit the trust of Subscriber certificates to the permitted uses in accordance with the Certificate Policy provisions of the corresponding issuing CA,

b) accept the TSL for usage only after observing the terms TSL acceptance defined in section 4.4,

c) be fully aware of applicable warranties and liabilities on acceptance and use of the TSL, and

d) notify any event or anomaly on a CA and its services which can be considered as a cause to revoke it, using the means defined in section 4.7.

9.5.5 Representations and Warranties of Other Participants

Not applicable.

9.6 Disclaimers of Warranties

MULTICERT refuses all service guarantees for which is not bound in the obligations set forth in this Policy.

9.7 Limitations of Liability

To the extent permitted by applicable law, this Policy limits the liabilities of the TSL Scheme Operator to the following:

a) MULTICERT is liable for causing damage to participants due to failure or delay beyond the defined deadlines in processing revocations or suspensions of CAs or services of CAs.

b) MULTICERT is liable for the conduct of trusted personnel holding functions necessary to provide TSL services.

c) MULTICERT is liable only for damages caused by improper use of the TSL, if it has not factored into the TSL the applicable usage limitations.

d) MULTICERT is not liable when a Relying Party overcomes the limits contained in the TSL as to its possible uses in accordance with the conditions established and communicated.

e) MULTICERT is not liable when a Relying Party does not verify the TSL in accordance with the defined rules, conditions and restrictions.

f) MULTICERT is not liable for losses or injuries:

f.1. for the services provided, in case of war, natural disasters or any other case of force majeure,

f.2. caused by TSL usages exceeding the limits established in this Policy,

f.3. caused by misuse or fraudulent use of the TSL or services provided by the CAs.

9.8 Indemnities

In accordance with applicable laws.

9.9 Term and Termination

9.9.1 Term

Documents relating to the TSL (including this Policy) become effective after approval by the Policy Administration and are only removed or changed by their order.

This Policy becomes effective from the moment of its publication in the TSL Scheme Operator repository.

This Policy is effective until expressly revoked by the issuing of a new version.

9.9.2 Termination

The Policy Administration may decide in favour of the elimination or amendment of a document relating to the TSL (including this Policy) if:

a) Its contents is considered incomplete, inaccurate or erroneous,

b) Its contents have been compromised.

In this case, the document shall be replaced by a new version.

This Policy shall be replaced by a new version independently of the committed changes, so it will always be applied in its entirety.

Should the Policy be replaced and withdrawn from the public repository, it shall be retained for 10 years.

9.9.3 Effect of Termination and Survival

After the Policy Administration decided in favour of eliminating a document related to the TSL, a 30-day period is considered to submit for approval a document replacement.

The obligations and restrictions provisioned in this Policy, in reference to audits, confidential information, obligations and liabilities of the TSL Scheme Operator, remain after being replaced or repealed to the extent that it does not oppose the new version.

9.10 Amendments

9.10.1 Procedure for Amendment

To amend this Policy, a formal request must be submitted to the Policy Administration (contacts in section 1.5), indicating the following information as a minimum:

- Identify the person who is submitting the amendment request,
- The reason for the request,
- The requested changes.

An assigned Policy Administration member reviews the request, verifies its relevance and undertakes the necessary updates to the document, resulting in a new draft version of the Policy. The new draft document is then available to all members of the Policy Administration and the affected parties (if any) for revision. Counting from the date of availability, the various parties have 15 working days to submit their comments. When that period ends, the Policy Administration members have 15 working days to review all comments received and, where deemed appropriate, incorporate them into the document. Afterwards, the document is approved and provided to the TSL Promoter for validation and approval. The publication of the new Policy finalizes the process and turns the changes effective.

9.10.2 Notification Mechanism and Period

In the event that the TSL Promoter considers that amendments to the Policy may affect the acceptability of the TSL for specific purposes, CAs shall be notified about the amendment and recommended to obtain and check the new Policy from the established repository.

9.11 Dispute Resolution Procedures

All complaints between the TSL participants shall be communicated by the party in dispute to the TSL Promoter in order to try to resolve it between the same parties.

To resolve any conflict that may arise with respect to this Policy, the parties undergo the Administrative Litigation Jurisdiction, waiving any other jurisdiction that may assist to them.

9.12 Governing Law

This Policy shall be governed by the laws of Belgium.

9.13 Compliance with Applicable Law

This Policy is subject to applicable national and European laws, rules, regulations, ordinances, decrees and orders including, but not limited to, restrictions on exporting or importing software, hardware or technical information.

9.14 Miscellaneous Provisions

9.14.1 Entire Agreement

All participants observe in its entirety the contents of the latest version of this Policy.

9.14.2 Assignment

In the event that one or more stipulations of this Policy are or deemed to be legally invalid, void or unclaimable, they should be considered as not applicable.

The previous situation is limited to cases where such stipulations are not considered essential. It is the responsibility of the TSL Promoter to perform the corresponding assessment.

9.14.3 Severability

Not applicable.

9.14.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable.

9.14.5 Force Majeure

To the extent permitted by applicable law, MULTICERT includes a force majeure protection clause covering its whole TSL activity.

9.15 Other Provisions

Not applicable.

Bibliography

ID	Document Number	Title	Issued by
[1]	EPC016-06	SEPA Core Direct Debit Scheme Rulebook (Annex VII: e-Mandates)	EPC
[2]	EPC109-08	e-Mandates e-Operating Model High Level Definition, version 1.5	EPC
[3]	EPC208-08	EPC e-Mandates e-Operating Model – Detailed Specification, version 1.1	EPC
[4]	EPC249-09	TSL Trust Body for EPC Approved Certification Authorities (CAs) in support of SEPA e Mandate Services Request for Proposals (RFP), version1.1	EPC
[5]	EPC292-09	Approval Scheme for EPC Approved CAs for e-Mandate Services, version 2.0	EPC
[6]	EPC306-07	e-Mandate Services Description v1.0 Approved	EPC
[7]	TS 102 231	Provision of harmonized Trust-service status information, version 3.1.2	ETSI
[8]	RFC 5280	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile	IETF
[9]	X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks	ITU-T
[10]	CWA 14167-1:2003	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements	CEN

Table 6 - Bibliography references