Time-Stamping Practice Statement

Policy

MULTICERT_PJ.CA3_24.1.1_0002_en

Project Identification: Multicert TSA

Access level: Public

Version: 10.0

Date: 17/11/2026

MULTICERT - Serviços de Certificação Electrónica, S.A.,
Alfrapark, Edifício E, Estrada de Alfragide, 67, 2610-008 AMADORA - PORTUGAL
Phone: +351 217 123 010

Document Identifier: MULTICERT_PJ.CA3_24.1.1_0002_en

Key-words: Time-Stamping Practice Statement

Type of document: Policy

Title: Time-Stamping Practice Statement

Original language: Portuguese

Publication language: English

Access level: Public

Date: 17/11/2026

Current version: 10.0

Project identification: Multicert TSA

Version history

Version	Date	Details	Author(s)
1.0	18/02/2009	Initial version	MULTICERT S.A.
1.1	04/08/2009	Document update, according to changes made on the Time-stamp platform	MULTICERT S.A.
1.2	06/06/2014	Revision	MULTICERT S.A.
2.0	01/08/2014	Approval	MULTICERT S.A.
2.1	15/07/2015	Revision	MULTICERT S.A.
3.0	22/03/2016	Approval	MULTICERT S.A.
3.1	16/04/2016	Inclusion of External Entities Obligations	MULTICERT S.A.
4.0	26/04/2017	Approval	MULTICERT S.A.
4.1	23/04/2018	Revision	MULTICERT S.A.
4.2	21/09/2021	Revision	Multicert S.A.
5.0	31/03/2022	Approval	Multicert S.A.
5.1	30/06/2023	Contacts revision, general revision	Multicert S.A.
6.0	01/07/2023	Approval	Multicert S.A.
6.1	01/07/2024	Revision	Multicert S.A.
7.0	01/07/2024	Approval	Multicert S.A.
7.1	12/02/2025	Revision	Multicert S.A.
8.0	13/02/2025	Approval	Multicert S.A.
8.1	16/09/2025	Revision	Multicert S.A.
9.0	15/12/2025	Approval	Multicert S.A.
9.1	17/11/2026	Inclusion of a statement of adherence to the CCADB policy	Multicert S.A.
10.0	17/11/2026	Approval	Multicert S.A.

Related documents

Document ID	Details	Author(s)
MULTICERT_PJ.ECRAIZ_427_en	MULTICERT Certification Practice Statement	MULTICERT S.A.

Summary

Time-Stamping Practice Statement 1
Summary 3
Introduction 5
1 Scope 6
2 References 7
3 Definitions and Acronyms 8
3.1 Definitions 8
3.2 Acronyms 10
4 General Concepts 11
4.1 General Policy Requirements Concepts 11
4.2 Time-Stamping Services 11
4.3 Time-Stamping Authority (TSA) 11
4.4 Subscriber 11
4.5 Time-Stamp Policy and TSA Practice Statement 11
5 Time-Stamp Policies 13
5.1 General Requirements 13
5.2 Policy Name and Identification 13
5.3 User Community and Applicability 13
6 Policies and Practices 14
6.1 Risk Assessment 14
6.2 Trust Service Practice Statement 14
6.2.1 Time-stamp Format 14
6.2.2 Time Precision 14
6.2.3 Service Limitations 14
6.2.4 Subscriber Obligations 14
6.2.5 Relying Parties Obligations 15
6.2.6 Time-stamp Verification 15
6.2.7 Applicable Legislation 16
6.2.8 Service Availability 16
6.3 Terms and Conditions 16
6.3.1 Applicable Trust Service Policy 16
6.3.2 Log Retention Period by the TSP 16
6.4 Information Security Policy 16
6.5 TSA Obligations 16
6.5.1 General 16
6.5.2 TSA`s Obligations to Subscribers 17
6.6 Information for the Relying Parties 17
7 TSA Management and Operation 18

Copyright © 2002-2025 MULTICERT - All rights reserved

7.1 Introduction 18
7.2 Internal Organization 18
7.3 Personnel Security 18
7.4 Asset Management 18
7.4.1 Media Management 18
7.5 Access Control 18
7.6 Cryptographic Controls 19
7.6.1 General 19
7.6.2 TSU Key Generation 19
7.6.3 TSU Private Key Protection 19
7.6.4 TSU Public Key Certificate 20
7.6.5 Rekeying TSU`s Key 20
7.6.6 Life Cycle Management of Signing Cryptographic Hardware 20
7.6.7 End of TSU Key Life Cycle 20
7.7 Time-stamping 20
7.7.1 Time-stamp Issuance 20
7.7.2 Clock Synchronization with UTC 21
7.8 Physical and Environmental Security 21
7.9 Operation Security 21
7.10 Network Security 22
7.11 Incident Management 22
7.12 Collection of Evidence 23
7.13 Business Continuity Management 23
7.14 TSA Termination and Termination Plans 24
7.15 Compliance 24
8 Additional Requirements for Qualified Electronic Time-stamps as per Regulation (EU) No 910/2014 25
8.1 TSU Public Key Certificate 25
8.2 TSA Issuing Non-Qualified and Qualified Electronic Time-stamps as per Regulation (EU) No 910/2014 25

Copyright © 2002-2025 MULTICERT - All rights reserved

Introduction

The infrastructure of Multicert's Time-Stamping Authority provides time-stamps and chronological validation mechanisms in accordance with national and European legislation, following the ETSI EN 319 421 standard, and is duly accredited by the Supervisory Body (https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5), as provided for in Portuguese and European law, thus being legally authorized to issue qualified time-stamps.

The time-stamps issued by Multicert's Time-Stamping Authority (TSA) provide the necessary mechanisms to prove that a datum (a set of information in electronic format) existed at the date the time-stamp was applied.

This CPS complies with the requirements of the CCADB Policy, version identified in section 2, available at https://www.ccadb.org/policy.

Copyright © 2002-2025 MULTICERT - All rights reserved

1 Scope

This document defines the policies and practices used by Multicert's Time-Stamping Authority, hereinafter referred to as TSA, in support of its activity of issuing time-stamps and providing chronological validation mechanisms.

The technical and procedural details of the TSA are described in this document, in addition to what is defined in Multicert's general Certification Practice Statement.

The time-stamps issued by Multicert comply with the ETSI EN 319 421 standard "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" and ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles."

Copyright © 2002-2025 MULTICERT - All rights reserved

2 References

Regulation (EU) n.º 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Regulation (EU) 2024/1183 of the European Parliament and of the Council, of 11 April 2024, amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

CCADB Policy, v2.1 (2026-03-20);

ETSI EN 319 401, v2.3.1 (2021-05) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1, v1.4.1 (2023-10) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2, v2.5.1 (2023-10) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

ETSI EN 319 421, v1.2.1 (2023-05) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

ETSI EN 319 422, v1.1.1 (2016-03) – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

ETSI TS 119 312, v1.5.1 (2024-12) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

Copyright © 2002-2025 MULTICERT - All rights reserved

3 Definitions and Acronyms

3.1 Definitions

Item	Definição
Digital Signature	Advanced electronic signature mode based on an asymmetric cryptographic system consisting of an algorithm or series of algorithms, through which a unique and interdependent pair of asymmetric keys, one of which is private and one is public, is generated and which allows the subscriber to use the private key to declare the authorship of the electronic document to which the signature is affixed and the agreement with its contents; it further allows the recipient to use the public key to verify that the signature was created by using the corresponding private key and if the electronic document was changed after being signed.
Qualified Electronic Signature	Digital signature or other advanced electronic signature mode that satisfies security requirements identical to those of the digital signature based on a qualified certificate and created through a secure signature creation device.
Digital Certificate	Electronic document that links signature verification data to its subscriber and confirms the identity of such subscriber.
Qualified Certificate	Electronic signature certificate, issued by a trusted service provider and which complies with the requirements set out in Annexes I, II III and IV to Regulation EU No. 910/2014.
Datum	Set of information in electronic format.
Trust Service Provider	Means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust

Copyright © 2002-2025 MULTICERT - All rights reserved

Item	Definição
	service provider.
Relying Party	Any natural person or legal entity that relies on a valid certificate.
Time-Stamp	Data in an electronic form that links other electronic data to a specific date/time, establishing proof that this data existed at that date/time.
Trust Service	Electronic service that consists of: a) Creating, verifying, and validating electronic signatures, electronic seals or time-stamps, registered electronic sending services, and certificates related to these services; or b) Creating, verifying, and validating certificates for website authentication; or c) Preserving the signatures, seals, or electronic certificates related to these services.
Time-stamping Service	Trust service for issuing time-stamps.
Subscriber	A natural person or legal entity to whom a certificate is issued and who is legally bound by a subscriber agreement or terms of use.
TSU (Time-stamping unit)	Set of hardware and software that is managed as a unit and has a single active time-stamp signature key at a given time.
UTC (Coordinated Universal Time)	Time scale based on the second, as defined in ITU-R Recommendation TF.460-5
Time-stamp validation	Statement from the certification authority, which certifies the date and time of creation, sending, or receipt of an electronic document.

Copyright © 2002-2025 MULTICERT - All rights reserved

3.2 Acronyms

Acronyms	Definition
BIPM	Bureau International des Poids et Mesures
CA	Certification Authority
CAB	Conformity Assessment Body
CP	Certificate Policy
CRL	Certificate Revocation List
DN	Distinguished Name
TSAPS	Time-Stamping Practice Statement
TSA	Time-Stamping Authority
GMT	Greenwich Mean Time
PKI	Public Key Infrastructure
CRL	Certificate Revocation List
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object identifier
TSP	Trust Service Provider
TSU	Time-stamping unit
UTC	Coordinated Universal Time

Copyright © 2002-2025 MULTICERT - All rights reserved

4 General Concepts

4.1 General Policy Requirements Concepts

This document considers the ETSI EN 319 401 standard as a reference for generic policy requirements.

The requirements of this TSAPS (Time-Stamping Practice Statement) are based on the use of public key cryptography, digital certificates, and reliable time sources.

This TSAPS should be consulted by Subscribers and Relying Parties to get accurate details on how Multicert's TSA operates.

4.2 Time-Stamping Services

The provision of time-stamping services is divided into the following service components, with the aim of classifying the requirements:

a) Time-stamping supply – this service component generates time stamps.

b) Time-stamping management – this service component monitors and controls the operation of time-stamping services to ensure that the service is provided according to what is specified by the TSA. This service component is responsible for the installation and uninstallation of the time-stamping supply service.

4.3 Time-Stamping Authority (TSA)

A Trust Service Provider that provides time-stamping services to the public is called a TSA.

The TSA is responsible for providing the time-stamping services identified in section 4.2, and is responsible for operating one or more TSUs (Time-stamping units) that create and sign on behalf of the TSA.

The TSA is a Trust Service Provider as described in ETSI EN 319 401, issuing time-stamps.

Multicert subjects the TSA to annual audits, carried out by an accredited CAB (Conformity Assessment Body). The report from this audit is sent to the Supervisory Body (National Security Office).

4.4 Subscriber

The Subscriber is an individual or corporate person who acquires the time-stamps produced by the TSA and accepts the terms and conditions of the TSA service.

4.5 Time-Stamp Policy and TSA Practice Statement

This section explains the roles of the TSA's policy and practice statement, without placing restrictions on its form.

The Time-Stamping Policy is a type of Trust Service Policy as specified in ETSI EN 319 401, applicable to Trust Service Providers that issue time-stamps.

Copyright © 2002-2025 MULTICERT - All rights reserved

This document specifies the time-stamping policy and practice statement of Multicert's TSA.

Copyright © 2002-2025 MULTICERT - All rights reserved

5 Time-Stamp Policies

5.1 General Requirements

This policy lays out a set of rules followed by Multicert when issuing time-stamps, supported by digital certificates, with an accuracy of 1 second or better relative to UTC.

5.2 Policy Name and Identification

The identifiers of the time-stamp policy specified in this document are:

- 1.3.6.1.4.1.25070.1.2.1.0.1 – identifier of TSA Practice Statement
- 1.3.6.1.4.1.25070.1.1.1.0.7 – identifier of Multicert Certification Practice Statement

By including this identifier, Multicert indicates compliance with the following additional time-stamp policies:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023)

policy-identifiers(1) best-practices-ts-policy (1)

The following identifiers are discontinued, but their information is now included in this document:

- 1.3.6.1.4.1.25070.1.1.1.2.0.1.1
- 1.3.6.1.4.1.25070.1.1.1.2.0.7

5.3 User Community and Applicability

This document can be used by public time-stamping services or time-stamping services used in a closed community.

Copyright © 2002-2025 MULTICERT - All rights reserved

6 Policies and Practices

6.1 Risk Assessment

Multicert carries out risk assessments at least once a year, which include, among other areas, the provision of time-stamping trust services. The risk assessment includes:

a) Identification and analysis of internal and external threats that may result in impacts;

b) Assessment of the impact of threats and the likelihood of their occurrence;

c) Definition of a Risk Treatment Plan, identifying the selected risk treatment measures, in order to reduce the identified risk to an acceptable level or eliminate it.

6.2 Trust Service Practice Statement

Multicert ensures the quality, performance, and operation of the time-stamping service through the implementation of security controls and policies.

The security controls and policies are regularly reviewed and audited by independent entities.

Additionally, to ensure compliance with the ETSI EN 319 421 standard, the measures outlined in the following subsections are implemented.

6.2.1 Time-stamp Format

The time-stamps issued by Multicert comply with RFC 3161. The service issues 2048-bit RSA time-stamps until 16/12/2025 and 3072-bit RSA time-stamps from 16/12/2025, using the SHA256 hash algorithm.

6.2.2 Time Precision

The time-stamping service uses a UTC appliance, synchronized via a GNSS system, with a fallback to configured UTC sources, which are always listed by the BIPM.

If the UTC source is not within the indicated accuracy, that is +/- 1 second, the time-stamp is not issued, and the TSA returns an error indicating that the time source is not available, as specified in RFC 3161.

6.2.3 Service Limitations

No stipulation.

6.2.4 Subscriber Obligations

It is the Subscriber’s duty to:

a) a) Not exceed the allowed number of time-stamp tokens purchased;

b) b) Be responsible for applying the time-stamps to documents using the URL provided by Multicert;

Copyright © 2002-2025 MULTICERT - All rights reserved

c) c) Not allow the service to be used by third parties;

d) d) Limit and appropriately use the time-stamps in accordance with current law and this document;

e) e) Request the issuance of time-stamps in accordance with RFC 3161;

f) f) Upon receiving the requested time-stamp, verify that the time-stamp has been correctly signed by Multicert's TSA;

g) g) Upon receiving the requested time-stamp, verify that the private key used for signing is valid (i.e., has not been compromised);

h) h) Not monitor, manipulate, or perform any 'reverse engineering' on the technical implementation (hardware and software) of the certification services without prior written authorization from Multicert.

6.2.5 Relying Parties Obligations

See section **Erro! A origem da referência não foi encontrada.**.

6.2.6 Time-stamp Verification

The verification of the time-stamp includes the checks described in the following subsections.

6.2.6.1 Time-stamp Issuer Verification

The TSA uses appropriate digital certificates to issue time-stamps. The digital certificates are issued by a Certification Authority whose digital certificate is published in the Multicert repository at https://pki.multicert.com.

6.2.6.2 Verification of the Time-Stamp Revocation Status

6.2.6.2.1 Verification of the Time-Stamp Revocation Status during the TSU Certificate Validity

The time-stamp is digitally signed by the TSU of the TSA of Multicert, using a digital certificate that is valid for 6 years. During the validity period of the TSU certificate, the validity of the signing private key can be checked through the revocation status of the TSU certificate, using the OCSP and CRL service access addresses listed in the digital certificate that issues the timestamps.

6.2.6.2.2 Verification of the Time-Stamp Revocation Status after the TSU Certificate Expiration

The time-stamp becomes unverifiable after the TSU certificate's validity period ends, since the TSA that issued the certificate no longer guarantees the publication of revocation data, including revocations due to the corresponding private key being compromised.

However, the time-stamp can still be verified after the TSU certificate's validity period ends, if at the time of verification it can be concluded that:

a) The TSU's private key was not compromised up to the end of its validity period (this can be checked via the CRL and/or OCSP);

Copyright © 2002-2025 MULTICERT - All rights reserved

b) The hash algorithms used in the time-stamp do not show collisions as of the verification date;
c) The signature algorithm and key size with which the time-stamp was signed are not cryptographically breakable at the time of verification.

If these conditions cannot be guaranteed, the validity of a time-stamp can be maintained by issuing a new time-stamp to protect the integrity of the previous time-stamp.

6.2.7 Applicable Legislation

This practice statement is managed and interpreted according to the applicable Portuguese and European legislation.

6.2.8 Service Availability

The security controls and measures implemented by Multicert are described in section 5 of the Multicert Certification Practices Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com.

6.3 Terms and Conditions

6.3.1 Applicable Trust Service Policy

This document represents the applicable trust service policy. For more information, check section 5.

6.3.2 Log Retention Period by the TSP

Multicert keeps the audit logs generated for a period of 7 years after the certificate's expiration date. Multicert makes these audit logs available to External Auditors during an audit or to the Supervisory Body, when requested.

6.4 Information Security Policy

Multicert has implemented an Information Security Policy, which is reviewed regularly or when changes occur that justify it.

Multicert's Information Security Policy is also framed within an Information Security Management System certified according to the ISO/IEC 27001 standard.

6.5 TSA Obligations

6.5.1 General

The TSA is responsible for:

a) Carrying out its operations in accordance with this Practice Statement;

b) Protecting its private time-stamping keys;

c) Issuing time-stamps in accordance with RFC 3161;

Copyright © 2002-2025 MULTICERT - All rights reserved

d) Issuing time-stamps that conform to the time-stamp request data provided by the Subscriber;

e) Ensuring the reliability of the time-stamp generation process and its delivery to the Subscriber;

f) Using reliable systems and products that are protected from any alteration and ensure the technical and cryptographic security of the time-stamp issuance processes;

g) Employing personnel with the necessary qualifications, knowledge, and experience to provide trust services;

h) Publishing this Practice Statement and applicable Policies in its public repository, ensuring access to current versions;

i) Cooperating with audits directed by the CAB;

j) Operating in accordance with applicable law;

k) In case of cessation of activity, inform the parties involved and within the timeframe indicated in Multicert's Certification Practices Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com;

l) Comply with the specifications contained in the Personal Data Protection legislation.

6.5.2 TSA`s Obligations to Subscribers

This document does not specify any additional obligations towards the Subscribers beyond those mentioned in section 6.5.1.

6.6 Information for the Relying Parties

Relying Parties are responsible for:

a) Limiting the reliability of time-stamps to the uses allowed for them, in accordance with applicable law and this document.

b) Verifying that the time-stamp was correctly signed.

c) Verifying that the private key used to sign the time-stamp has not been compromised up to the moment of verification.

d) Checking the status of time-stamps, according to section 6.2.6.

e) Taking responsibility for the correct verification of time-stamps;

f) Reporting any event or unusual situation related to the time-stamp, using the means that Multicert publishes in its Certification Practices Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com.

Copyright © 2002-2025 MULTICERT - All rights reserved

7 TSA Management and Operation

7.1 Introduction

Multicert has security policies and operational procedures in place to keep the service safe.

7.2 Internal Organization

For the proper operation of the time-stamping validation service, Multicert maintains a set of internal documentation that specifies operational controls related to staff security, access control, risk assessment, among others. This documentation is audited by independent auditors confirming the service's compliance with the ETSI EN 319 421 standard.

The legal entity that provides the time-stamping validation service is MULTICERT – Electronic Certification Services, S.A.

The TSA uses systems for quality and information security management appropriate to the time-stamping validation services provided.

The TSA is operated by people with the knowledge and training necessary to perform the service.

7.3 Personnel Security

The staff performing duties at TSA meet the requirements set out in section 5.3 of the Multicert Certification Practice Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com.

7.4 Asset Management

Multicert has implemented security controls to protect the resources and information resources used in the time-stamp validation service.

7.4.1 Media Management

The media used in the time-stamp validation service is handled safely to keep it protected against damage, theft, unauthorized access, or obsolescence, and in compliance with applicable practices according to the classification of the information contained in the media.

Multicert has established procedures to ensure the protection of the media against obsolescence and deterioration. The destruction of media also follows defined procedures to ensure its safe disposal and prevent unauthorized access to the information contained.

7.5 Access Control

Access to TSA systems is limited only to authorized individuals. Specifically:

a) Access privileges follow the principle of 'least privileges,' with individuals having access only to what is necessary to perform their duties;

Copyright © 2002-2025 MULTICERT - All rights reserved

b) Access is modified or removed in a timely manner, according to individuals' allocation in work groups;

c) Access to information and systems is restricted according to the Access Control Management Policy;

d) Security controls are implemented to segregate the functions of different work groups and the permissions they have in the systems;

e) Authentication mechanisms are implemented for access to information and systems;

f) Audit logs of activities performed in the systems are kept, ensuring accountability for actions carried out by members of the work groups;

g) Security controls are in place to protect resources from unauthorized access to sensitive information, and these security controls are applied throughout the information lifecycle.

7.6 Cryptographic Controls

7.6.1 General

Multicert uses several private keys in the TSA service. A private key is used to issue the time-stamp certificates that are used by the TSUs. All private keys are stored in cryptographic hardware evaluated according to FIPS 140-2 level 3, FIPS 140-3 level 3 and/or Common Criteria EAL 4+ requirements.

7.6.2 TSU Key Generation

The generation of the TSA's cryptographic keys is carried out at Multicert's secure facilities (in accordance with section 5.1 of Multicert's Certification Practices Statement (MULTICERT_PJ.ECRAIZ_427)) by the members of the Working Groups, composed of authorized personnel, in a planned and audited ceremony following established operating procedures. All key generation ceremonies are recorded, dated, and signed by the Working Group members involved in the ceremony.

The cryptographic hardware used for TSA key generation meets FIPS 140-2 level 3, FIPS 140-3 level 3, and/or Common Criteria EAL 4+ requirements, and handles key maintenance, storage, and all operations involving cryptographic keys exclusively using the cryptographic hardware. Access to critical keys is protected by security policies, role separation among the Working Groups, as well as through limited user access rules.

The TSU key generation algorithm, the signature key size, and the signing algorithm used to sign the time-stamps follow the specifications of the ETSI TS 119 312 standard.

7.6.3 TSU Private Key Protection

The private key that signs the TSU is generated and handled within cryptographic hardware that meets FIPS 140-2 level 3, FIPS 140-3 level 3, and/or Common Criteria EAL 4+ requirements.

Backups of the TSU private keys are made, and performing and storing these backups is done only by members of authorized Working Groups, requiring the involvement of different Working Groups.
Backups of the TSU private keys are always made using a direct cryptographic hardware-to-hardware connection.

Copyright © 2002-2025 MULTICERT - All rights reserved

7.6.4 TSU Public Key Certificate

Multicert ensures the integrity and authenticity of the TSU public key in the following way:

a) The verification public key for the TSU signature is publicly available through a digital certificate. The digital certificate can be found in the Multicert repository at https://pki.multicert.com.

b) The digital certificate containing the TSU signature verification public key is issued by a previously audited Certification Authority, using as a minimum criterion the ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 421, and ETSI EN 319 422 standards, and is included in the European trusted list available at https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5.

7.6.5 Rekeying TSU`s Key

The validity period of the TSU certificate is not longer than the time period during which the chosen algorithm and key size are recognized as secure (see section 7.6.2).

7.6.6 Life Cycle Management of Signing Cryptographic Hardware

The cryptographic hardware is inspected during the commissioning process to ensure its compliance and to check that there is no evidence of it having been tampered with.

The installation, activation, and duplication of the TSU's signing keys on the cryptographic hardware are carried out by members of various authorized Working Groups, with these operations only being performed at Multicert's secure facilities (see section 5.1 of the Multicert Certification Practices Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com).

The disposal of cryptographic hardware that contains the TSU's private signing keys is carried out following defined procedures using techniques that make key recovery practically impossible.

7.6.7 End of TSU Key Life Cycle

The validity of the private keys used never exceeds the validity of the certificates issued using those same keys.

7.7 Time-stamping

Multicert issues qualified time-stamps that comply with the time-stamp profile defined in the ETSI EN 319 422 standard.

7.7.1 Time-stamp Issuance

Time-stamps are issued securely, specifically:

a) The TSU uses time values in the time-stamps that can be traced back to the actual time distributed by UTC labs listed in the BIPM.

b) The time included in the time-stamp is synchronized with UTC within an accuracy of +/- 1 second or better.

Copyright © 2002-2025 MULTICERT - All rights reserved

c) Time-stamps are not issued if the TSA's clock is outside the accuracy indicated in b), until the clock is synchronized again.

d) Time-stamps are signed with a key generated exclusively for this purpose.

e) Time-stamps are not issued using a TSU private key that has expired.

7.7.2 Clock Synchronization with UTC

The TSA clock is synchronized with UTC via NTP. In particular:

a) The clock calibration is maintained within the accuracy indicated in section 7.7.1, point b).
b) The TSU clock is protected against attacks that could result in an undetected alteration of the clock that would take it out of calibration.
c) The accuracy of the TSU clock is monitored. If the clock accuracy is outside the parameters indicated in section 7.7.1, point b), the TSA does not issue time-stamps as indicated in section 7.7.1, point c).
d) Clock synchronization is maintained when a leap second is scheduled, as notified by the competent authority. The adjustment to account for the leap second is made in the last minute of the day on which the leap second is scheduled. A record of the exact time the change occurred is created.

7.8 Physical and Environmental Security

Multicert maintains physical and environmental security policies for the systems used in TSA services, which cover physical access control, protection against natural disasters, fire prevention and protection, protection against power and communication failures, protection against water leaks, protection against theft or unauthorized access attempts, and disaster recovery. The provisions in section 5.1 of the Multicert Certification Practice Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com apply.

Controls are in place to protect the equipment, information, media, and software related to TSA services.

7.9 Operation Security

Multicert has a set of security controls in place that ensure the quality and availability of the service.

In particular, these controls include:

a) Analyzing security requirements when designing and specifying requirements for TSA systems.

b) Implementing change control procedures applied to releases, modifications, and urgent fixes of operational software.

c) Protecting the integrity of Multicert's information systems against viruses, malicious software, or unauthorized access.

d) Defining and implementing procedures for the workgroups performing functions in service delivery.

e) Specification of procedures to ensure that security patches are applied within a reasonable timeframe after they have been released. A security patch does not need to

Copyright © 2002-2025 MULTICERT - All rights reserved

be applied if it introduces vulnerabilities or instabilities that outweigh the benefit of applying it. In that case, the reason why the security patch was not applied is documented.

f) Monitoring the necessary resource capacity, as well as future capacity needs projections, to ensure the required availability of power and memory.

7.10 Network Security

Multicert protects its network and systems from attacks.

In particular:

a) The network is segmented considering the functional, logical, and physical relationships of trusted systems and services.

b) The same security controls are applied to all systems within the same secure zone.

c) Access and communications between zones are restricted to only what is necessary for TSP operations. Unnecessary connections and services are prohibited or disabled, and the established rules are regularly reviewed.

d) Critical systems for TSP operations are located in secure zones.

e) The IT systems administration network is separated from the TSP operational network. Systems used for administering the security policy implementation are not used for other purposes.

f) Production systems are separated from systems in other environments.

g) Communication between different trust systems can only be established through reliable channels that are logically separate from other communication channels, and provide secure identification of their endpoints and protection of channel data against alteration or disclosure.

h) The external network connection to the internet is redundant to ensure service availability in case of failure.

i) Vulnerability scans of public and private IP addresses are carried out quarterly, and evidence is recorded that the scans were performed by people with the knowledge, tools, code of ethics, and independence necessary to deliver a reliable report.

j) Penetration tests are carried out annually on the systems when the setup is done and after applying upgrades to the infrastructure or modifications that Multicert considers relevant. Evidence is recorded showing that the penetration tests were conducted by people with the knowledge, tools, code of ethics, and independence required to deliver a reliable report.

k) Controls (like firewalls) are implemented to protect Multicert's internal domains from unauthorized access, including access by Subscribers or third parties, and to prevent all unnecessary protocols and access to Multicert's operations as a TSP.

l) TSU systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in TSA operations.

7.11 Incident Management

The activities of IT systems, as well as their usage and service requests, are monitored.

Copyright © 2002-2025 MULTICERT - All rights reserved

In particular:

a) The monitoring of activities takes into account the criticality of the information present. At a minimum, the following events are monitored:
   - Start-up and shutdown of logging functions (logs).
   - Availability and use of necessary services on the TSP network.
   - Audit logs.

b) Abnormal activities that indicate a potential security breach, including intrusions into trusted services networks, are detected and reported through alarms.

c) An incident management process is in place that is triggered in case of incidents. The process includes:
   - Identification and response to detected incidents.
   - People responsible for identifying and resolving incidents.
   - Notification of third parties, according to applicable law.
   - Identification of root causes and lessons learned.

d) If critical vulnerabilities are discovered that have not yet been addressed, they are dealt with within 48 hours of being found.

e) For each vulnerability, taking into account its potential impact:
   - A mitigation plan is created and implemented; or
   - The reason why the vulnerability does not require mitigation is documented based on facts.

7.12 Collection of Evidence

Multicert records and keeps audit logs accessible, in accordance with section 5.4 of the Multicert Certification Practice Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com.

Additionally, all events related to the following are recorded:

a) The lifecycle of TSU keys.

b) The lifecycle of TSU certificates.

c) The synchronization of the TSU clock, including information related to normal recalibration or synchronization of the clocks used in time-stamps.

d) The detection of clock synchronization loss.

7.13 Business Continuity Management

Multicert has regularly defined and tested a Business Continuity Plan, which includes the timely resumption of activities as a Trust Service Provider.

This plan includes recovery in case of compromise or suspected compromise of the TSU signing private key or loss of TSU clock calibration, and the procedures to be carried out include:

a) Describing and communicating the compromise that occurred to Subscribers and Relying Parties.

Copyright © 2002-2025 MULTICERT - All rights reserved

b) Stopping the issuance of time-stamps until the compromise has been resolved.

c) Providing information to Subscribers and Relying Parties to help them identify time-stamps that may have been affected by the compromise, unless this information would compromise TSA users' privacy or the security of TSA services.

7.14 TSA Termination and Termination Plans

In case the TSA ceases its activities, Multicert will take the following actions:

a) Inform the Supervisory Body, Subscribers, and other entities with which there are agreements.

b) Publish information about the cessation of activity for the Relying Parties.

c) Revoke the TSU certificates.

d) Destroy or permanently prevent the use of the TSA's private keys.

e) Ensure the transfer for retention of all information related to the TSA's activities, namely the TSA key, TSU certificates, availability of CRLs, stored documentation, repositories, and log storage within the period defined in section 5.5.2 of Multicert's Certification Practice Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com.

7.15 Compliance

Multicert ensures compliance with applicable laws and regulations, with annual audits carried out by an independent entity (CAB) to verify compliance, in accordance with section 8 of Multicert's Certification Practice Statement (MULTICERT_PJ.ECRAIZ_427) available at https://pki.multicert.com.

In particular, Multicert's TSA complies with:

a) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014;
b) Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April 2024;
c) Decree-Law No. 12/2021;
d) ETSI EN 319 401;
e) ETSI EN 319 421;
f) ETSI EN 319 422.

Copyright © 2002-2025 MULTICERT - All rights reserved

8 Additional Requirements for Qualified Electronic Time-stamps as per Regulation (EU) No 910/2014

8.1 TSU Public Key Certificate

Qualified time-stamp certificates are issued by Multicert Certification Authorities that operate according to ETSI EN 319 411-2.

8.2 TSA Issuing Non-Qualified and Qualified Electronic Time-stamps as per Regulation (EU) No 910/2014

Multicert does not issue non-qualified time-stamps. Qualified time-stamps are issued as specified in section 8.1.

Copyright © 2002-2025 MULTICERT - All rights reserved

Approval

Nuno Ponte (Management Working Group)



Digitally signed by
[Assinatura Qualificada]
Nuno Miguel Arieiro
Rodrigues da Ponte
Date: 2026.11.23
08:53:09 Z

Copyright © 2002-2025 MULTICERT - All rights reserved