TIMESTAMP CERTIFICATE POLICY

Global Trusted Sign

Document Reference: PL14_GTS_V11

Document Classification: Public

Date: July 4th, 2023

Document OID: 1.3.6.1.4.1.50302.1.1.2.3.1.0

Table of Contents

1. Introduction

a) Purpose

The purpose of this document is to present the Timestamp Certificate Policy of Global Trusted Sign Timestamping Authority, as a qualified service provider within the framework of Regulation No. 910/2014 (hereinafter referred to as GTS TSA).

b) Target Audience

This document should be read by:

- Human resources assigned to the GTS TSA working groups;
- Third parties in charge of auditing the GTS TSA;
- All the general public.

c) Document Structure

This document follows the structure defined and proposed by the PKIX working group (Public-Key Infrastructure X.509), of the IETF (Internet Engineering Task Force), in document RFC 3647. Within the scope of this Certificate Policy, it is assumed that the reader is familiar with the concepts of cryptography, public key infrastructures, and electronic signature. In case this situation does not occur, we recommend the previous study of the referred topics, thus enabling a better understanding of this policy.

1.1. Overview

This document focuses on the definition of profiles of Timestamp Certificates issued the GTS TSA (Global Trusted Sign Timestamping Authority), enabling the assurance of liability of the Chronological Validation also available in the GTS PKI. The certificates issued by the GTS TSA contain a reference to the GTS TSA Certification Practice Statement (TSA CPS) in order to allow relying parties and other interested entities or persons to find information about the certificate and the policies followed by the issuing authority.

1.2. Document Name and Identification

This document is the “Timestamp Certificate Policy”. This Certificate Policy (CP) is represented on a certificate through a unique number referred to as “Object Identifier” (OID):

Document information	
Document Name	Timestamp Certificate Policy
Document Version	11.0

Document Status	Approved
OID	1.3.6.1.4.1.50302.1.1.2.3.1.0
Date of Issue	July 4th, 2023
Validity	July 4th, 2024
Location	https://pki.globaltrustedsign.com/index.html

Note: Regular updates to this document are made whenever justified.

1.2.1. Revisions

Version Number	Creation	Approval	Reason
11	04-07-2023	04-07-2023	Annual verification of the document and update of values associated with telephone contacts
	Security Administration	**Management Group**	
	Débora Sofia Vieira Rodrigues	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: DÉBORA SOFIA VIEIRA RODRIGUES Data: 04-07-2023 12:44:18		

1.2.2. Relevant Dates

Version ID	Version Date	Reason for new version
Version 1	14-08-2017	To present the Timestamp Certificate Policy of the Global Trusted Sign Timestamping Authority, as a qualified service provider under regulation 910/2014
Version 2	13-02-2018	Update of the certificate "O" field
Version 3	26-07-2018	Update of OID validity
Version 4	10-01-2019	Update of OID validity
Version 5	31-01-2019	Update of the certificate attributes
Version 6	06-03-2020	Update of OID
Version 7	17-09-2020	Update of registration of employees of the GTS Trust Group
Version 8	06-05-2021	Update of document structure according to RFC 3647
Version 9	22-07-2022	Annual verification
Version 10	15-02-2023	Update of the PKI hierarchy and document structure
Version 11	04-07-2023	Annual verification of the document and update of values associated with telephone contacts

1.3. PKI Participants

1.3.1. Certification Authorities

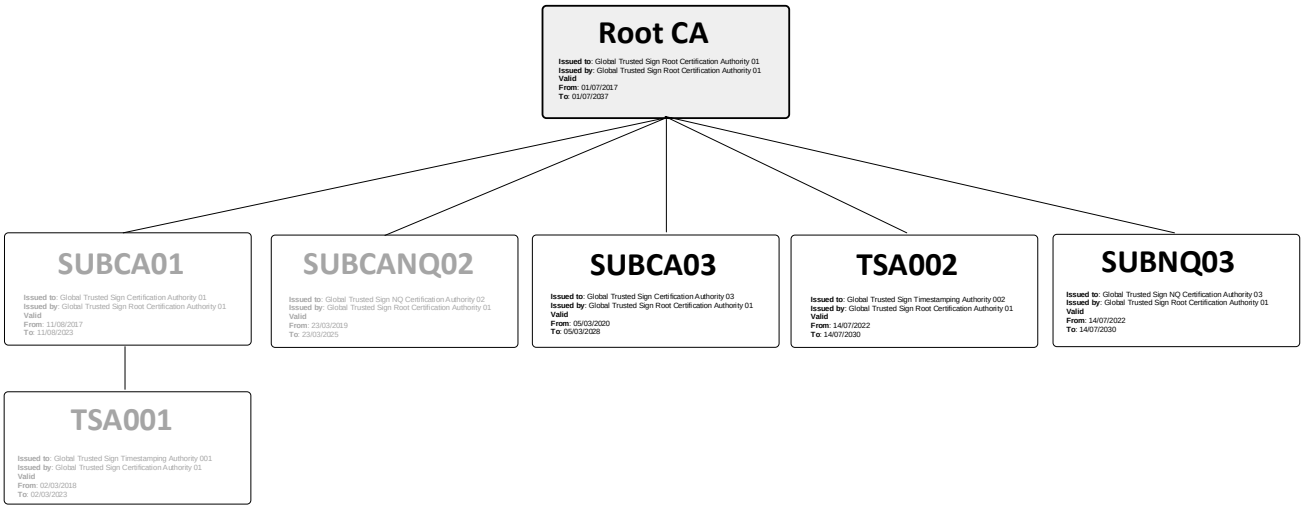
ACIN-iCloud Solutions, acts as the Certification Authority, with the following corporate data:

Social denomination: ACIN-iCloud Solutions, Lda.

VAT Number: 511 135 610

Address: Estrada Regional 104, Nº 42 A, 9350-203 Ribeira Brava
Phone Number: Local: 707 451 451[1] / International +351 291 957 888[2]
Web Page: www.acin.pt

GTS, as a qualified trust service provider, has a trust hierarchy accredited by the National Security Office -*Gabinete Nacional de Segurança* - (http://www.gns.gov.pt/trusted-lists.aspx), in accordance with the Portuguese and European legislation. The GTS trust hierarchy has a group of devices, applications, human resources and procedures required to implement diverse available certification services and to ensure the life cycle of certificates described in this document. The GTS trust hierarchy is composed by the GTS Root Certification Authority (GTS ROOT CA), the GTS Certification Authorities (GTS CA 01 – SUBCA01 and GTS CA 03 – SUBCA03), the GTS Non-Qualified Certification Authority (GTS NQ CA – SUBCANQ02 and SUBNQ03) and the GTS Time Stamps Certification Authority (GTS TSA GTS – TSA001 and TSA002).



Legend:
1 – GTS Root CA – GTS Root Certification Authority
2 – SUBCA01 - Certification Authority
3 – TSA001 - GTS Timestamping Certification Authority
4 – SUBCANQ02 - GTS Non-Qualified Certification Authority
5 – SUBCA03– GTS Certification Authority
6 – TSA002 – GTS Timestamping Certification Authority
7 – SUBNQ03 – GTS Non-Qualified Certification Authority

[1]Maximum amount to be paid per minute: 0.09€ (+VAT) for calls from fixed networks and 0.13€ (+VAT) for calls from mobile networks.
[2] Coast of an international call to a fixed network, according to the current rate.

a) GTS Timestamping Certification Authority (GTS TSA)

The GTS TSA is a chronological validation certification authority, authorised to issue qualified timestamps. Monitoring the issuance service of timestamps is intended to detect any major diversion larger than the requirements established by standard ETSI EN ETSI EN 319 421. All offsets between devices that support timestamps issuance service will be properly monitored, with the aim of identifying significant alarms that will be used to take corrective measures. The GTS TSA is responsible for operating in one or more TSU (*time-stamping unit*) to create and to sign timestamps on behalf of GTS. Each TSU has a distinct signature key, whose clock, used to issue timestamps is synchronized, is synchronised not only with the GTS's own atomic clock, but also, for redundancy purposes, with two other sources accredited in accordance with ETSI EN 319 421.

GTS TSA - TSA001 certificate:

Certificate Information	
Distinguished Name	CN = Global Trusted Sign Timestamping Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Signature Algorithm	Sha256RSA
Serie Number	04 bd 81 30 e4 ae 61 40 5a 99 43 db 7a 72 4f 47
Validity	02/03/2018 a 02/03/2023
Thumbprint	21 16 db 77 7e 72 fd 57 61 2a 24 27 8f d2 05 c8 bc fd a3 98
Issuer	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

GTS TSA - TSA002 certificate:

Certificate Information	
Distinguished Name	CN = Global Trusted Sign Timestamping Authority 002, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT
Signature Algorithm	sha256RSA
Serie Number	21 ee 9d 30 24 e9 0c 7e 62 cf f9 ac 3f f1 0c 08
Validity	14/07/2022 a 14/07/2030
Thumbprint	bf e9 50 86 06 35 80 b8 91 ea 42 e3 c1 e6 70 43 b5 3f 11 e4
Issuer	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

1.3.2. Registration Authorities

The Registration Authority (RA) is the entity responsible for approving the distinguished names (DN) of the holders of certificates and evaluates the veracity of the documents and identity of the holders of the requests. Based on this evaluation, it accepts or rejects the request.

Additionally, the RA has the authority to approve the revocation of certificates.

The Global Trusted Sign Registration Authorities comply with the requirements set out in this document and are subject to independent External Audits, as well as to Internal Audits carried out on a regular basis at Global Trusted Sign.

The issuance of the digital certificates implies the acceptance of the Terms and Conditions of the certificates – F031.

a) Internal Registration Authority

Within the scope of the Global Trusted Sign Certification Authority, the registration authority is implemented by its internal services, which have the responsibility to validate the required data, in accordance with each specific Policy of the services provided by Global Trusted Sign.

b) External Registration Authority

Global Trusted Sign does not have External Registry Authorities, as no contract exists with third parties to validate the domain of the SSL certificates and the identity of the advanced and qualified certificates.

1.3.3. Subscribers

Within the scope of this certificate policy, subscribers/holders are all final users to whom certificates have been attributed by the GTS PKI. The holders of certificates issued by GTS are considered those whose name is inscribed in the " Subject" field of the certificate and use it, as well as the respective private key in accordance with that set forth in the various certificate policies described in this document, with certificates being issued for the following categories of holders:

- Natural or legal person;
- Legal person (organizations);
- Services (computers, firewalls, etc.);
- The members of the working groups, namely the Security Administration, act as subscribers, taking responsibility for the correct use of the certificate, as well as for the protection and safeguard of the respective private key.

1.3.4. Relying Parties

The relying parties or recipients are natural persons, entities or equipment that trust in the validity of the mechanisms and procedures used in the association process of the name of the holder with its public key, that is, they trust that the certificate really corresponds to whom it says it belongs to. In this document, a relying party is considered to be that which trusts the content, validity and applicability of the certificate issued by the GTS PKI.

1.3.5. Other Participants

a) Supervisory Authority

The Supervisory Authority is the competent entity for the accreditation and supervision of certification authorities providing qualified trust services. At the national level, this function is performed by the National Security Office -*Gabinete Nacional de Segurança* (GNS)-. The supervisory authority contributes to the trust on qualified certificates, due to the functions exercised on the issuing Certificate Authority (CA). As part of its duties regarding Certification Authorities, the supervisory authority has the following tasks:

- **Notice of intent:** procedure to approve trust services conducted by qualified service providers, based on an assessment made of several parameters, such as physical security, hardware, software, access and operational procedures;
- **Conformity assessment body:** as a competent body to assess the conformity on trust services by qualified service providers;

- **Monitoring:** inspections are carried out to confirm that qualified and trusted service providers and trusted services comply with the requirements established on the EU Regulation No. 910/2014 of the European Parliament and of the Council.

b) External Entities

Activities of service providers that support GTS in its capacity of a qualified trust service provider are based on a contract to ensure the formal assignment of functions and responsibilities of each party, as well as the compliance with policies and practices established by GTS.

c) Conformity Assessment Body

The Conformity Assessment Body (CAB) is the entity defined in article 2, No. 13, of EU Regulation No. 765/2008, accredited in the terms of that regulation as being competent to assess the conformity of qualified trust service providers and trust services provided by them.

1.4. Certificate Usage

Certificates issued by the GTS PKI are used, by the different holders, systems, applications, mechanisms and protocols, in order to guarantee the following security services, namely:

- Authentication;
- Confidentiality;
- Integrity;
- Data Privacy;
- Non-Repudiation;
- Authenticity.

These services are obtained through public key cryptography, using the trust structure provided by the GTS PKI. Relying Parties can verify the chain of trust of a certificate issued by the GTS TSA, thus guaranteeing the authenticity and identity of the holder. Qualified certificates issued by the GTS TSA in accordance with this CP are qualified certificates in accordance with the requirements set forth in Regulation (EU) 910/2014.

1.4.1. Appropriate Certificate Uses

Timestamps are issued at the request of subscribers in accordance with ETSI EN 319 421 and comply with the requirements imposed by RFC 3161. They are also used by Relying Parties to validate the association of date/time with the datum and, for that purpose, they must:

- Verify that the timestamp has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of verification. During the validity of the TSU certificate, the validity of the signature key can be verified by checking the revocation status of the TSU certificate;

- Take into account the limitations on the use of timestamps as defined in this certificate practice statement and in the certificate policy;

- Take into consideration any other precautions applicable to the use of timestamps defined, for example, in agreements.

Note: The requirements and rules defined in this document apply to all timestamps issued by the GTS TSA.

1.4.2. Prohibited Certificate Uses

Timestamps cannot be used for any other purpose outside the context of the aforementioned uses except for the possibility that they can be used in other contexts when legally permitted by the applicable legislation.

1.5. Policy Administration

1.5.1. Organization Administering the Document

The management of the GTS TSA Certificate Policy is responsibility of the GTS Trust Group.

1.5.2. Contact Person

	GTS Trusted Group
Managers	Tolentino de Deus Faria Pereira José Luís de Sousa
Address	ACIN iCloud Solutions, Lda. Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira – Portugal
General e-mail	info@globaltrustedsign.com
Report e-mail	report@globaltrustedsign.com
Web Page	https://www.globaltrustedsign.com
Phone Numbers	National: 707 451 451 [1] International: + 351 291 957 888 [2] (Portuguese - Option 1 / English - Option 2; GTS - Option 6) [1] Maximum amount to be paid per minute: 0.09€ (+VAT) for calls from fixed networks and 0.13€ (+VAT) for calls from mobile networks. [2] Cost of an international call to a fixed network, according to the current rate.

When any of the grounds for revocation set out in point 4.9.1. is identified, it should be communicated to the above-mentioned contacts.

1.5.3. Person Determining CPS suitability for the policy

The Certificate Policy (CP) should be internally applied, as well as audited by the Audit working group in order to ensure its conformity. This audit should produce a report, which must be submitted to the GTS TSA Management Group, for its approval.

1.5.4. CPS Approval Procedures

The validation of this CP and all corrections or updates are performed by the GTS Security Administration. All corrections or updates are published as new versions of this CP, replacing any CP previously defined. The GTS Security Administration is responsible for determining when the changes on the CP will result in a change on the object identifiers (OID) of the CP. After validation, the CP is submitted to the GTS Trust Group, which is responsible for the approval and authorisation of the changes in this type of document.

1.6. Definitions and Acronyms

1.6.1. Definitions

Definitions	
Term	**Definition**
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign
Advanced electronic signature	An electronic signature which meets the following requirements: a) It is uniquely linked to the signatory; b) It is capable of identifying the signatory; c) It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and d) It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable
Authentication	Electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed
Certificate	Structure of electronic data signed by a certification service provider, which links the holder to the data of validation of signature that confirms his/her identity.
Certificate for Electronic Signature	Electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person
Certificate for Website Authentication	Attestation that makes possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued
Certificate for Electronic Seal	Electronic attestation that links e-seal validation data to a legal person and confirms the name of that person
Qualified Certificate for Electronic Signature	Certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the European Regulation 910/2014.
Qualified Certificate for Website Authentication	Certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV of the European Regulation 910/2014.
Qualified Certificate for Electronic Seals	Certificate for electronic seals, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of the European Regulation 910/2014.
Private Key	Element of the asymmetric key pairs meant to be known only to its holder, on which the digital signature is added on the electronic document, or which deciphers a previously encrypted electronic document, with the corresponding public key.
Public Key	Element of the asymmetric key pairs meant to be released, on which the digital signature affixed on the electronic document is verified, or an electronic document is encrypted to be transmitted to the holder of the key pairs.

Definitions	
Term	**Definition**
Accreditation	An act whereby a service provider is recognised or requesting that the activity of the certification entity may be exercised in accordance with requirements set by European Regulation 910/2014.
Creator of a Seal	Legal person who creates an electronic seal.
Personal Identification Data	Set of data enabling to determine the identity of a natural or legal person, or that of a natural person representing a legal person.
Validation Data	Data that is used to validate an electronic signature or an e-seal.
Electronic Seal Creation Data	Unique group of data used by the creator of the e-seal to create an e-seal.
Electronic Signature Creation Data	Unique group of data used by the signatory to create an electronic signature.
Electronic Signature Creation Device	Configured *software* or *hardware*, used to create an electronic signature
Electronic Seal Creation Device	Configured *software* or *hardware* used to create an electronic seal.
Qualified Electronic Signature Creation Device	Electronic signature creation device that meets the requirements laid down in Annex II of the European Regulation 910/2014.
Qualified Electronic Seals Creation Device	Electronic seal creation device that meets *mutatis mutandis* the requirements laid down in Annex II of the European Regulation 910/2014.
Electronic Document	Any content stored in electronic form, in particular text or sound, visual or audio-visual recording.
Electronic Address	Identification of computer equipment, proper to receive and file electronic documents.
Certification Authority	Natural or legal person, accredited as a qualified service provider by the supervisory authority.
Registration Authority	Entity that approves Distinct Names (DN) of subordinated entities and, by assessing the request, approves or rejects the request.
Supervisory Authority	Appointed entity for the accreditation and inspection of certification authorities.
Hash Function	Operation done by a group of data in any size, so that the result is another fixed size group of data independent from its original size and is uniquely linked to initial data and ensures it is impossible to obtain distinct messages that manage the result when applying that function.
Hash or Fingerprint	Fixed size result obtained after the application of a hash function to a message that complies the requirement of being uniquely linked to initial data.
HSM	Cryptographic security module used to store keys and cryptographic operations in a secure way.
Electronic Identification	The process of using personal identification data in electronic form, representing uniquely either a natural or legal person, or a natural person representing a legal person.

Definitions	
Term	**Definition**
Public Key Infrastructure	Hardware, software, persons, processes and policies structure that uses digital signature technology to provide trusted third parties a verifiable association between the public component of an asymmetric pair of keys and a specific signatory.
CRL	Revoked certificates list created and signed by the Certification Authority (CA) that issued the certificates. A certificate is introduced on the list when has been revoked (for example, by suspecting the key's compromise). In certain circumstances, the CA can divide a CRL into smaller CRLs.
Electronic Identification Mean	A material and/or immaterial unit containing personal identification data and which is used for authentication for an online service.
OID	Unique alphanumeric/numeric identifier registered according to an ISO norm, to refer to a specific object or to a specific class of objects.
Conformity Assessment Body	A body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides.
Public Body	National, regional or local government body, a body subject to public law or an association formed by one or more of those entities or by a body subject to public law, or a private entity authorised by, at least, one of those authorities, bodies or associations as being of public interest, under the current mandate.
Relying Party	Relying parties or final recipients are natural or legal people that trust in the validity of mechanisms and procedures used in the linking process of a time stamp to a datum. In other words, they rely on the time stamp's accuracy.
Certificate Policy	Group of rules that indicate the certificate's applicability to a specific community and/or application class with common security requirements.
Trust Service Provider	Natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
Qualified Trust Service Provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Product	Hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services.
Electronic Seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

Definitions	
Term	**Definition**
Advanced Electronic Seal	Electronic seal which meets the following requirements: a) it is uniquely linked to the creator of the seal b) it is capable of identifying the creator of the seal c) it is created using e-seal creation data that the creator of the seal can, with a high level of confidence under its control, use for e-seal creation; and d) d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
Qualified Electronic Seal	Advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.
Qualified Timestamp	An electronic timestamp which meets following requirements: a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably b) it is based on an accurate time source linked to Coordinated Universal Time; and c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.
Timestamps	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
Trust Service	Electronic service normally provided for remuneration which consists of: a) the creation, verification, and validation of electronic signatures, e-seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or b) the creation, verification and validation of certificates for website authentication; or c) the preservation of electronic signatures, seals or certificates related to those services.
Qualified Trust Service	Trust service that meets the applicable requirements laid down in the European Regulation 910/2014.
Electronic Registered Delivery Service	Service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

Definitions	
Term	**Definition**
Qualified Electronic Registered Delivery Service	Electronic registered delivery service which meets the following requirements: a) they are provided by one or more qualified trust service provider(s); b) they ensure with a high level of confidence the identification of the sender; c) they ensure the identification of the addressee before the delivery of the data; d) the sending and receiving of data is secured by an advanced electronic signature or an advanced e-seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.
Signatory	Natural person that creates an electronic signature.
Electronic Identification System	Electronic identification system under which electronic identification means are produced for natural or legal people or for natural people in representation of legal people.
Holder	See Signatory.
User	Natural or legal person that uses electronic identification or a trust service.
Validation	Process of verifying and confirming that an electronic signature or a seal is valid.
Chronological Validation	Declaration of a TSA that certifies the date and hour of creation, expedition or reception of an electronic document.
High Security Zone	Access controlled area in which an entry point is limited to authorised staff duly accredited and visitors properly accompanied. High security zones must be closed around its perimeter and watched 24 hours a day, 7 days a week, by security personnel, other personnel or by electronic means.

1.6.2. Acronyms

Acronyms	
C	Country
CN	Common Name
DN	Distinguished Name
CPS	Certification Practice Statement
RD	Regulatory Decree
CA	Certification Authority
RA	Registry Authority
GNS	National Security Office -Gabinete Nacional de Segurança-
GTS	Global Trusted Sign
HSM	Hardware Secure Module
CRL	Certificate Revocation List
O	Organization
OU	Organization Unit
OID	Object Identifier
CP	Certificate Policy
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SSL/TLS	Secure Sockets Layer / Transport Layer Security

1.6.3. References

- ✓ DP03_GTS - GTS Timestamp Authority Certification Practice Statement;
- ✓ Regulation (EU) No 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;
- ✓ ETSI 319 421, v.1.1.1 - Electronic Signatures and Infrastructures (ESI) Policy and Security Requirements for Trust Service Providers Issuing Time Stamps;
- ✓ ETSI 319 422, v.1.1.1 - Electronic Signatures and Infrastructures (ESI) Time-stamping protocol and time-stamp token profiles;
- ✓ RFC 3161 – Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP);
- ✓ RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;
- ✓ CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4.

1.6.4. Conventions

No stipulation.

2. Publication and Repository Responsibilities

2.1. Repositories

The GTS CA provides a repository, in web environment, with information regarding practices adopted and the status of certificates issued, namely:

a) GTS Root Certification Authority (GTS ROOT CA)

- GTS ROOT CA Certificate;
- GTS ROOT CA Certificate Revocation List (CRL);
- GTS ROOT CA Certification Practice Statement (CPS);
- GTS ROOT CA Certificate Policies (CP);

- Other relevant information.

b) GTS Certification Authority (GTS CA)

- GTS CA Certificate;
- GTS CA Certificate Revocation List (CRL);
- GTS CA Certification Practice Statement (CPS);
- GTS CA Certificate Policies;
- Other relevant information.

c) GTS Timestamping Certification Authority (GTS TSA)

- GTS TSA Certificate;
- GTS TSA Certification Practice Statement (CPS);
- GTS TSA Certificates Policies;
- Other relevant information.

d) GTS Non-Qualified Certification Authority (GTS NQ CA)

- GTS NQ CA Certificate;
- GTS NQ CA Certificate Revocation List (CRL);
- GTS NQ CA Certification Practice Statement (CPS);
- GTS NQ CA Certificates Policies;
- Other relevant information.

2.2. Publication of information

The repository of the different certification authorities can be accessed 24x7 at https://pki.globaltrustedsign.com/index.html and at https://pki02.globaltrustedsign.com/index.html. The repository will be updated when an amendment is made to any published documents.

2.3. Time or Frequency of Publication

The GTS TSA conducts the following publications, with the following frequency of publication:

- The GTS TSA certificate is published after its issuance;
- The CRL is published quarterly;
- New versions or amendments of CPS and/or respective Certificate Policies (CP), are published after approval by the Management Group.

2.4. Access Controls on Repositories

The following security access control mechanisms have been implemented:

- Any amendments to the information published in the repository is done through formal procedures of document management;
- The technological infrastructure that supports the repository and its publications is in conformity with the good practices of information security, including physical requirements, as well as the management by a team with skills required to perform those activities;
- It is guaranteed that the access to the information contained in the repository is carried out, only and exclusively, in read mode. To that end, security mechanisms have been implemented to ensure that only authorised persons may write or modify the information contained in the repositories.

3. Identification and Authentication

3.1. Naming

The allocation of names follows the convention established in the Certification Practice Statement, (DP03).

3.1.1. Types of Names

The GTS TSA certificate is identified by a Distinguished Name (DN), according to what is set in standard X.509. The unique name of the timestamp certificate is identified by the following components:

Attribute	Code	Value
Country	C	PT
Organization	O	ACIN iCloud Solutions, Lda
Organization Unit	OU	Global Trusted Sign
Common Name	CN	Global Trusted Sign Timestamping Authority 001

3.1.2. Need for Names to be Meaningful

The GTS TSA ensures that the names used in the certificates it issues identify in a significant and clear manner their holders, ensuring that the DN used is appropriate for a certain holder and that the "***Common Name***" component of the DN represents it in a manner that can be easily identified by the

interested parties. The GTS TSA ensures that any ***Common Name*** field in the Subject DN of the certificate is equal to one of the ***Subject Alternative Names*** FQDN, which was validated using at least one of the procedures specified in section 3.2.2.4 of the Baseline Requirements CA/B Forum.

3.1.3. Anonymity or Pseudonymity of Subscribers

The GTS TSA does not allow the anonymity of holders in the certificate issuance process.

3.1.4. Rules for Interpreting Various Names Forms

The rules used by the GTS TSA to interpret the name format follow that established in *RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* thus guaranteeing that all *DirectoryString* attributes of the issuer and subject fields of the certificate are encoded in a UTF8String, with the exception of the country and serialnumber attributes which are encoded in a *PrintableString.*

3.1.5. Uniqueness of Names

In the GTS TSA, there are controls that ensure that the DN and the *KeyUsage* extension content are unique, unambiguous and related only to one entity, thus guaranteeing the rejection of certificates issued by it that, having the same unique name, identify distinct entities.

3.1.6. Recognition, Authentication and Role of Trademarks

DNs issued by the GTS TSA are unique for each holder and take into account the registered trademarks, not allowing the deliberate use of registered names whose entity cannot prove it has the right to the trademark, and may refuse to issue the certificate with registered trademark names if it concludes that another identification is more convenient. Before issuing the certificate, during the authentication procedure, the entity/holder shall present documents that demonstrate the right to use the requested DN.

3.2. Initial Identity Validation

In order for the qualified certificates of the Certification Authorities to be issued in the GTS trust hierarchy, it is mandatory that the GTS TSA verifies the request and the parameters associated to them.

3.2.1. Method to Prove Possession of Private Key

In cases in which the GTS TSA is not the entity responsible for generating the cryptographic pair of keys to attribute to the user, the latter, before issuing it, shall assure that the user possesses the private key corresponding to the public key included in the certificate request.
The method of proof shall necessarily be more complex and precise according to the importance of the type of certificate requested, being documented in the Certificate Policy of the certificate in question.

3.2.2. Authentication of Organization and Domain Identity

DNs issued by the GTS TSA take into account the trademarks, not allowing the deliberate use of registered names whose entity cannot prove it has the right to the trademark, and may refuse to issue the certificate with registered trademarks if it concludes that another identification is more convenient.

For certificates that include the identity of an organization, the data on the legal person shall be validated using one of the forms described in the CPS.

3.2.2.1. Identity

Before issuing and making available a certificate issued for a legal or natural person with the attribute of association with an entity, it is necessary to authenticate the data regarding the creation and legal person of the entity.

For these certificates, the identification of the entity is required in all cases, for which the RA shall require the relevant documentation depending on the type of entity.

The relevant documentation may be found on the Globaltrustedsign website, in the corresponding certificate information section.

In the case of entities located outside the Portuguese territory, the documentation to be submitted will be that of the Official Registry of the respective country, duly apostilled and officially translated into Portuguese or English, whenever there are doubts regarding the documentation or the entity.

This verification is done through an analysis of the legal regime applicable to the applicant entity and through consultation of the records of the business activity of the market or through the physical delivery of the notarial deeds that prove all the information.

In addition, it is also verified:

- That the data or documents provided are within the validity period.

- That the legal existence of the organization is at least 1 year.
- That they are not eradicated companies in countries where there is a government ban on doing business or on a BCFT risk related list.

3.2.2.2. DBA/Tradename

See section 3.1.6.

3.2.2.3. Verification of Country

See section 3.2.2.

3.2.2.4. Validation of Domain Authorization or Control

For each domain, it is confirmed that the applicant has control over that domain by means of a verification at the registry at https://www.whois.net and/or https://www.dns.pt

3.2.2.5. Authentication for an IP address

For each IP address, it is confirmed that the applicant has control over that address by a verification in the registry at https://www.ripe.net or https://whois.arin.net/

3.2.2.6. Wildcard Domain

GTS does not issue Wildcard certificates

3.2.2.7. Data Source Accuracy

GTS has a list of reliable sources to analyse the data prior to issuing the certificates.

3.2.2.8. CAA Records

The verification of CAA Records is done through the tool https://www.entrustdatacard.com/products/categories/ssl-certificates/caa-tool
For further information please see section 4.2.1.

3.2.3. Authentication of Individual Identity

GTS will verify the data in the registration process carried out by the subscriber, in the respective service request form available at www.globaltrustedsign.com, in accordance with that described in section 3.2.2.1.

3.2.4. Non-Verified Subscriber Information

All the information provided by the subscriber is verified.

3.2.5. Validation of Authority

See Organization and Domain Identity Authentication, section 3.2.2 and Individual Identity Authentication, section 3.2.3.

3.2.6. Criteria for Interoperation or Certification

Certificates issued on the GTS PKI are issued under a single trust hierarchy.
In order to ensure total interoperability between applications that use digital certificates, it is recommended to use only alphanumeric characters with o graphic accentuation, space, underline, minus symbol and full stop ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') on X.500 directory inputs.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Many public key infrastructures allow automatic updating of certificates for a subscriber before the expiration of the validity date of the current certificate. This action is known as routine renewal and is possible at the moment when there is already a trust relationship with the underwriter. The renewal is treated as a new issuance request by the GTS TSA.

3.3.2. Identification and Authentication for Re-Key after Revocation

The renewal is treated like a new issuance request by the GTS TSA. GTS requires the subscriber to use the same authentication details used in the original certificate request.

3.4. Identification and Authentication for Revocation Request

The revocation request must comply with the conditions described in detail in section 4.10.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

A request to the GTS TSA for the issuance of certificates begins with the completion of a form, designed for each type of certificate supported and with the acceptance of the terms and conditions established by the GTS TSA.

4.1.1. Who Can Submit a Certificate Application

Certificate subscription requests may be submitted by:

- The certificate holder;
- A representative of the certificate holder, duly authorized by a power of attorney to that aim;
- A legal person who is the holder of the certificate;
- A GTS representative.

4.1.2. Enrollment Process and Responsibilities

After requesting the timestamping service, a process of validation of the information and identity of the holder and, when applicable, requesting entity is initiated. This process is carried out by the Registry Administrators, with the purpose of verifying the authenticity of the data provided, depending on the type of certificate requested. GTS does not use external registration entities to provide the registration service. A certificate request does not imply its obtainment in case the applicant does not meet the requirements established in this CP. Accepted or rejected submitted requests quell be stored and preserved by a minimum period of 7 years, in accordance with CAB Forum section 5.5.2.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

As soon as GTS receives the certificate issuance request form, as well as the necessary information for issuing the request, it shall proceed to validate all information provided in order to verify the authenticity of the data. The identification domain of the GTS TSA in the CAA records is globaltrustedsign.com. The GTS TSA limits the reuse of the supporting information for the renewal of the certificate, in accordance with point “11.14.3- Age of Validated Data” of the Guidelines for the Issuance and Management of Extended Validation Certificates do CA/ Browser Forum.

4.2.2. Approval or Rejection of Certificate Applications

Certificate requests shall only be accepted if all request data is authentic. In case of information contained in the evaluation process, the application shall be rejected, and the party responsible for the same shall be informed.

4.2.3. Time to Process Certificate Applications

GTS provides the certificates after validation of the signed request and successful payment, according to the general terms and conditions available in the public area.

4.3. Certificate Issuance

The certificate issuance process is carried out by the GTS TSA Registration Administrators through a specific procedure for that purpose. The certificates are issued through the interaction of the GTS TSA with a cryptographic module in hardware (*Hardware Secure Module* - HSM). The issued certificate begins its validity at the moment it is issued.

4.3.1. CA Actions during Certificate Issuance

Access to the certificate information is available in the private area of the platform, through login, as well as through the email associated with the registration and service request.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

The subscriber of the certificate is notified via electronic mail, and the public key certificate is sent through this channel.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Before the delivery of the public key certificate, the subscriber and holder must agree the certificate use conditions, only after that, the certificate will be considered as accepted. Regarding the issued certificate, the subscriber must be aware of the following issues:

- Knowledge of the features and content of the certificate;
- Knowledge of rights and responsibilities.

4.4.2. Publication of the Certificate by the CA

The GTS TSA does not publish the list of issued certificates.

4.4.3. Notification of Certificate Issuance by the CA to other Entities

The GTS TSA does not notify other entities about their issuance.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Certificate holders use their private key, only and exclusively, for the intended purpose (in accordance with the provisions in the field of the certificate "*keyUsage*") and always for legal purposes. The holder always is responsible for the use of the certificate.
The use of the certificate is only allowed, and applicable to the type of certificate:

- To whoever is designated in the *Subject* field of the certificate;
- After accepting the terms and conditions associated with the type of certificate;
- Whilst the certificate is valid and is not included in the CRL of GTS TSA.

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties shall use software that complies with the X.509 standards and shall only trust the certificate if it is not expired or revoked. The GTS TSA supplies in this CP information about the appropriate services available to verify the validity status of the certificate, such as OCSP and CRL.

4.6. Certificate Renewal

To renew the certificate, and if the functions and information for which the initial certificate was issued are maintained, it is only required to request the renewal of that certificate with the same data and make a renewal payment following the instructions that will be sent by GTS. This process requires a new generation of a key pair and of the respective certificate.

4.6.1. Circumstance for Certificate Renewal

If a holder intends to renew a certificate, a procedure is triggered for each one of the following cases:

Renewal Reason	Renewal Procedure
The certificate was revoked	(*i*) A new pair of keys is generated, and consequently a new certificate is issued with the same fields, except the public key.
The holder intends to extent the validity of the certificate	(*i*) The old certificate is revoked. (*ii*) A new pair of keys is generated, and consequently a new certificate is issued with the same fields, except the public key.
The Certificate original information has been modified	(*i*) The old certificate is revoked. (*ii*) A new pair of keys is generated, and consequently a new certificate is issued with the amendments, including the new public key.

The renewal of certificates follows the procedures of initial identification and authentication, resulting in the generation of new pairs of keys.

4.6.2. Who may Request Renewal

The Subscribers/Holders under the conditions established in point 4.6.1 may request the renewal of certificates.

4.6.3. Processing Certificate Renewal Request

The processing of the certificate renewal request is carried out as described in point 4.6.1.

4.6.4. Notification of New Certificate Issuance to Subscriber

The GTS TSA notifies the Subscriber, usually by email, within a reasonable time after the certificate has been issued, and may use any reliable mechanism to deliver the certificate to the Subscriber.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6. Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.7. Certificate Re-Key

4.7.1. Circumstance for Certificate Re-Key

The Re-Key process of a certificate consists in creating a new certificate with a new public key, maintaining, however, the same information in the "*Distinguished Name*" and "*Subject Alternative Name*" fields of the previous certificate.

4.7.2. Who may Request Certification of a New Public Key

See section 4.1.

4.7.3. Processing Certificate Re-Key Requests

See section 4.2.

4.7.4. Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.1.

4.7.6. Publication of the Re-Keyed Certificate by the CA

See section 4.4.2.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.8. Certificate Modification

Certificate modification is a process through which the certificate is issued to a Subscriber or Sponsor maintaining the same keys, with changes only in the certificate information. The modification of certificates is not supported by the GTS TSA.

4.8.1. Circumstances for Certificate Modification

No stipulation.

4.8.2. Who May Request a Certificate Modification

No stipulation.

4.8.3. Processing Certificate Modification Requests

No stipulation.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of the Modified Certificate by the CA

No stipulation.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9. Certificate Revocation and Suspension

The revocation of certificates is a mechanism used when, for any reason, certificates are not reliable, before the originally intended end period. In practice, certificates revocation is an action through which

the certificate ceases its validity before the expiration period, losing, in this way, its functionality. The suspension of certificates is not supported by the GTS TSA.

4.9.1. Circumstances for Revocation

A certificate can be revoked due to any of the following reasons:

- Cease of activities;
- Theft, loss, destruction or deterioration of the supporting device of the certificates;
- Inaccuracies in data supplied;
- Risk or suspicion of risk of the holder private key;
- Risk or suspicion of risk of the certificate access password;
- Risk or suspicion of risk of the GTS TSA private keys;
- Breach of responsibilities under the CPS by the GTS TSA or by the holder;
- Whenever there are credible reasons to suppose that certification services are under risk, so there are doubts about the certificate reliability;
- By legal or administrative resolution;
- Whenever it is determined that, for some reason, certificates were not issued in accordance with the GTS Certificate Policy or Certification Practices Statement;
- Whenever the GTS TSA receives notification or has implied knowledge of any circumstance that indicates that the certificate's email address is no longer legally authorised;
- Use of the certificate for abusive activities.

4.9.1.1. Reasons for Revoking a Subscriber Certificate

a) A certificate can be revoked due to any of the following reasons:

- The Subscriber requests in writing the revocation of the Certificate;
- The Subscriber notifies that the original certificate request was not authorised and does not grant authorisation retroactively;
- Cease of functions;
- Theft, loss, destruction or deterioration of the supporting device of the certificates;
- Inaccuracies in data supplied;
- Risk or suspicion of risk of the holder private key;
- Risk or suspicion of risk of the certificate access password;
- Risk or suspicion of risk of the GTS ROOT CA private keys;
- Breach of responsibilities under the CPS by the GTS ROOT CA or by the holder;

- When the GTS TSA is aware of a demonstrated or proven method that can easily calculate the Private Key of the Subscriber based on the Public Key in the Certificate (as a Debian weak key, according to https://wiki.debian.org/SSLkeys;
- When the GTS TSA obtains evidence that the validation of domain authorisation or control for any Fully Qualified Domain Name or IP address in the Certificate should not be relied upon;
- Whenever there are credible reasons to suppose that certification services are under risk, so there are doubts about the certificate reliability;
- By legal or administrative resolution;
- Whenever it is determined that, for some reason, certificates were not issued in accordance with the GTS Certificate Policy or Certification Practices Statement;
- Whenever the GTS TSA receives notification or has implied knowledge of any circumstance that indicates that the certificate's email address is no longer legally authorised;
- Use of the certificate for abusive activities.

b) The CA may revoke a certificate within 24 hours, but shall revoke it within 5 days for one or more of the following reasons:

- The Certificate does not comply with the requirements of Section 6.1.5 and Section 6.1.6;
- The GTS ROOT CA obtains evidence that the Certificate has been misused;
- The GTS ROOT CA is informed that a subscriber has breached one or more of its material obligations under the terms and conditions;
- The GTS ROOT CA is aware of any circumstances indicating that the use of a Fully Qualified Domain Name or IP address in the Certificate, which is no longer legally authorized (e.g., a court or arbitrator has revoked the right of a Domain Name Subscriber to use the Domain Name, a relevant licensing or services agreement between the Domain Name registry and the Applicant has been terminated, or the Domain Name registry has not renewed the Domain Name);
- The GTS ROOT CA is informed that a wildcard Certificate has been used to authenticate a fraudulently misleading fully qualified subordinate domain name;
- The GTS ROOT CA becomes aware of a material change in the information contained in the Certificate;
- The GTS ROOT CA is aware that the Certificate has not been issued in accordance with these Requirements or the CA Certificate Policy or Certification Practices Statement;
- The GTS ROOT CA determines or becomes aware that any information contained in the Certificate is inaccurate;

- The right of the GTS ROOT CA to issue certificates under these requirements expires, is revoked or terminated unless the GTS ROOT CA has resolved to maintain the CRL/OCSP Repository;
- Revocation is required by the GTS ROOT CA Certificate Policy and/or Certification Practice Statement; or
- The GTS TSA is informed of a demonstrated or proven method that exposes the Private Key of the subscriber upon compromise or if there is clear evidence that the specific method used to generate the Private Key was incorrect or defective.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate.

The issuing CA shall revoke a GTS CA Certificate within seven (7) days if one or more of the following situations occur:

- The GTS CA requests the revocation in writing;
- The GTS CA notifies the Issuing CA that the original certificate request was not authorized and does not grant authorization retroactively;
- The GTS CA obtains evidence that the GTS CA Private Key corresponding to the Public Key in the Certificate has suffered a Key Compromise or no longer meets the requirements of Section 6.1.5 and Section 6.1.6;
- The GTS CA obtains evidence that the Certificate has been misused;
- The GTS CA is informed that the Certificate has not been issued in accordance with or that the Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
- The GTS CA determines that any information contained in the certificate is inaccurate or misleading;
- The GTS ROOT CA or the GTS CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The right of the Issuing CA or Subordinate CA to issue certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
- Revocation is required by the Certificate Policy and/or Certification Practices Statement of the Issuing CA

4.9.2. Who can Request Revocation

Revocation can be legitimately requested by any of the following parties:

- The Certificate holder;
- The Certification Authority or Requesting Entity of the certificate of the subordinate entity;
- GTS, when aware that:
  - Data contained in the certificate does not correspond to reality;
  - The certificate is not in the possession of its holder;
- The Supervisory Authority;
- A relying party, when proves that the certificate has been used for purposes other than those intended to be used.

4.9.3. Procedure for Revocation Request

Any Revocation Request must be submitted through the service available for that purpose at https://www.globaltrustedsign.com. The GTS TSA will process the revocation request in the next 24 hours after the revocation request has been received. During that period of time, the identity and authenticity of the applicant will be verified.

4.9.4. Revocation Request Grace Period

The revocation request grace period is the time available for the Subscriber to take the necessary actions to request the revocation of a certificate over which there is suspicion of compromising the key, discovery of inaccurate information contained in the certificate, or outdated information. In this case, the Subscriber shall request the revocation within 24 hours after its detection.

4.9.5. Time within which CA must Process the Revocation Request

After confirmation of the identity and authenticity of the applicant, the GTS TSP will proceed, within 60 minutes, to change the certificate status to revoked.

4.9.6. Revocation Checking Requirement for Relying Parties

Before relying on the information contained in a certificate, the Relying Party shall validate the appropriateness of the certificate for the intended purpose and ensure that the certificate is valid. To verify the status of the certificate, the Relying Parties need to consult the OCSP or CRL responses identified in each certificate.

4.9.7. CRL Issuance Frequency (if applicable)

The status of certificates issued by the GTS CA can be checked by consulting the CRL, which is issued whenever there is a revocation of the certificates issued or, in the absence of changes in the status of the certificates, and it is downloaded in less than 10 seconds. In order to guarantee its availability, the CRL is released in the following repositories:

- https://pki.globaltrustedsign.com/download/crl/root/gts_root_crl.crl;
- https://pki02.globaltrustedsign.com/download/crl/root/gts_root_crl.crl

4.9.8. Maximum Latency for CRLs (if applicable)

GTS has sufficient resources to guarantee normal operating conditions, namely a response time, for CRL and OCSP, less or equal to 10 seconds.

4.9.9. Online Revocation/Status Checking Availability

Global Trusted Sign has an OCSP validation service for the status of the certificates online. This service can be accessed at http://ocsp.globaltrustedsign.com

4.9.10. Online Revocation Checking Requirements

Before using a certificate, the relying parties have the responsibility of verifying the status of all the certificates, through the CRL or a verification server of the online status (via OCSP).
The CRL can be accessed at https://pki.globaltrustedsign.com/index.html, guaranteeing its availability 24 hours per day, 7 days per week, except in the occurrence of a scheduled maintenance stoppage and duly communicated to the parties involved.
The end of the subscription of a certificate occurs when the validity period is expired or the certificate is revoked, according to RFC 3647. The service updates OCSP responses with a periodicity of 10m as defined in the ***nextupdate*** field.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Re-Key Compromise

In addition to the reasons mentioned in section 4.9.1 of this Certificate Policy, the parties may use the email report@globaltrustedsign.com to demonstrate the compromising of the private key of the subscribed certificates.

4.9.13. Circumstances for Suspension

No stipulation.

4.9.14. Who can Request Suspension?

No stipulation.

4.9.15. Procedure for Suspension Request

No stipulation.

4.9.16. Limits on Suspension Period

No stipulation.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

The status of issued certificates is publicly available using CRL and the OCSP service.

4.10.2. Service Availability

The certificate status service is available 24 hours per day, 7 days per week. If a certificate is revoked, it does not remain in the CRL after the expiration date.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

The end of a certificate subscription occurs when the validity period is expired or the certificate is revoked, according to RFC 3647.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

The GTS TSA retains its private key and the private keys of all its customers through an HSM stored in a secure environment.

- They are archived internally in secure environments and for long periods of time;
- They are generated and stored in HSM and their transfer to other media or devices is not possible;
- The private keys of the GTS TSA have at least one backup copy, with the same security level as the original key and are subject to backup copies;
- They are stored in encrypted form in HSM.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

See section 4.12.1.

5. Management, Operational and Physical Controls

5.1. Physical Security Controls

5.1.1. Site Location and Construction

GTS was designed to provide a safe environment capable of protecting the systems that support the activities of the Certification Authority. GTS activities are conducted in a room located in a high security zone, within a building which guarantees the existence of various levels of security, accessible only to the people required for the performance of its trust activities. GTS also guarantees that its high security zones possess all the features, as well as the necessary mechanisms to guarantee security conditions related to:

- Physical location and type of construction, with masonry, concrete or brick walls;
- Ceiling and floor with similar construction to the walls;
- No windows;
- Security door, with steel plate, with fixed hinges and shoulder also in steel, with security lock electronically operated, fire-resistant features and functionality anti-panic;
- Physical access to the premises;
- Power and air conditioning;
- Exposure to water / flooding;
- Prevention and protection against incidents/disasters such as fire, flood and similar;
- Waste disposal;

- Safeguard of database backups.

5.1.2. Physical Access

In order to offer confidentiality, integrity and availability of information to the technological infrastructure, GTS is organised into six security levels:

- Level 1;
- Level 2;
- Level 3;
- Level 4;
- Level 5;
- Level 6.

Security Level 1 is identified by a large part of the infrastructure area. The first security perimeter found is the reception area of the building, where the staff of the organization is subject to a biometric system and visitors are subject to appropriate registration by the reception staff. This area is also equipped with CCTV cameras capable of monitoring all access points to the building. The next security area is called Level 2. This level is located in a floor of the building for this purpose and represents the corridor between level 01, the systems room (Level 3) and the TSP's room (Level 4), being that, to access this area, a positive authentication in the passage of an access control by the TSP's trust groups is required. In the case of visitors (auditors and maintenance) will be provided an access card for authentication in access controls. These cards only validate access with the prior authentication of members that perform organic functions within the TSP structure. The area represented by security level 3 comprises the antechamber area and the systems room. The main function of the antechamber zone is to prevent direct passage from Security Level 2 to Level 4. Access to these areas is intended only for authorised personnel, while visitors (auditors and maintenance) can only access when accompanied by the TSP Trusted Groups. Entry or exit made at this level is only allowed after a positive identification in the access controls, and these identifications are based on the biometric factor. The access control system is managed through software that controls all access points to the infrastructure. Access to Security Level 4 is performed from an access controls device. Access is only allowed after the positive identification of two employees from different trust groups. Two identification mechanisms are used simultaneously, biometrics and PIN code. Level 5 of security is materialised by the Security Vault located within Level 4, where the smartcards of the TSP Administrators/Operators are located for access to the certificate lifecycle management systems. Access to them is only authorised to the members of the trust group with functions established in the TSP's organization and with access to the services provided by the TSP. It should also be noted that the Security Vault is approved according to the EN 1143-1 standard. The last security level, Level 6, is defined by the individual compartments within

the Security Vault (Level 5), where the devices to access the functionalities of the TSP system are located. Each compartment identifies an authorized individual and with functions established in the TSP's organization, to which only the individual can have access.

5.1.3. Power and Air Conditioning

The GTS safe environment has redundant equipment, which guarantees operating conditions 24 hours a day / 7 days a week, of:

- Uninterruptible continuous power supply with sufficient power to autonomously maintain the power grid during periods of power failure and to protect the equipment from electrical fluctuations that could damage it (the redundant equipment consists of uninterruptible power supply batteries, and diesel electricity generators);
- Refrigeration/ventilation/air conditioning which control the temperature and humidity levels, ensuring suitable conditions for the correct operation of all the electronic and mechanical equipment present within the environment. A temperature sensor activates a GSM alert whenever the temperature reaches abnormal values. This GSM alert consists of phone calls with a pre-recorded message to the maintenance team members.

5.1.4. Water Exposures

The high security zones have the appropriate mechanisms installed (flood detectors) to minimise the impact of floods on the GTS systems.

5.1.5. Fire Prevention and Protection

The GTS safe environment has installed the necessary mechanisms to prevent and extinguish fires or other incidents derived from flames or fumes. These mechanisms comply with existing regulations:

- Fire detection and alarm systems are installed on the various physical levels of security;
- Fixed and mobile fire extinguishing equipment is available, placed in strategic and easily accessible locations so that it can be quickly used at the beginning of a fire and successfully extinguished;
- There are well defined emergency procedures in case of fire.

5.1.6. Media Storage

Media with sensitive information are stored securely, in vaults and in accordance with the type of media and classification of the information. Access to these areas is restricted to duly authorised persons.

5.1.7. Waste Disposal

At the end of their life cycle, documents and paper materials containing critical information should be disposed of by effective methods that do not allow for their reconstruction.
Other storage equipment (hard disks and the like) shall be properly cleaned, so that it is not possible to recover any information through secure formatting, or physical destruction of the equipment. In the case of cryptographic peripherals, these shall be destroyed in accordance with the instructions and recommendations of the respective manufacturers.

5.1.8. Off-Site Backup

All backup copies are kept in a secure environment in external facilities.

5.2. Procedural Controls

The GTS digital certificate issuing activity, as a qualified certification authority, requires compliance with a set of European standards. These same standards define a set of working groups, with distinct competences, activities and rules, which shall be guaranteed by GTS. In the trust functions are included all personnel with access to the CA certification systems and that in practice may materially affect:

- Manipulation of subscriber information and validation of Certificate issuance information;
- Functions of the life cycle of the certificates;
- Configuration and maintenance of the certification systems;

Within the scope of its organizational structure, the following are considered to be trust functions, and are divided and differentiated by the nature of their activity, whether they are software for digital certification. Each of them is entrusted with the following responsibilities depending on their scope.

5.2.1. Trusted Roles

a) System Administration Working Group (AdmSist)

Responsible for the installation, configuration and maintenance of the systems, but with controlled access to security-related settings. This group has the following responsibilities:

- Production environment management;
- Installation, configuration, maintenance of systems and network with controlled access to application components settings;
- Management of the performance of systems that support GTS activities, to ensure that the infrastructure is always available and operational, and forecasting future needs that may arise from GTS activities and their costs;
- Management of hardware and software incidents and failures;

- Restitution of the system through backup copies, when necessary;
- Execution and maintenance of documents (procedures) related to the execution of its functions;
- Safeguard of artefacts under its custody.

b) Security Administration Working Group (AdmSeg)

Global responsible for security systems, in particular, for the management and implementation of rules and safety practices within the scope of services provided by GTS. This group has the following responsibilities:

- Definition of documentation related to GTS information security practices;
- Definition of procedures related to cryptographic keys management;
- To ensure that all GTS documentation is updated, adapted to the reality and stored in a secure manner, depending on their classification;
- Management of the implementation of security practices and policies, including logical and physical access control;
- Management of risks associated with services provided by GTS;
- Security events monitoring and related alarm management;
- Participation and response to security incidents;
- Safeguard of artefacts under its custody.

c) Systems Operation Working Group (OpSist)

Responsible for routine functioning of the trust system, being authorized to make security backups and its recovery. This group has the following responsibilities:

- Systems daily operation;
- Routine operations;
- Security backups;
- Safeguard of artefacts under its custody.

d) Registry Administration Working Group (AdmReg)

Responsible for the approval of the issuance, suspension and revocation of digital certificates (qualified signature, electronic seals, website authentication and timestamps certificates). This group has the following responsibilities:

- Certificate issuance and revocation;

- Submission of *Certificate Signing Request* (CSR) for the implementation of registration processes;
- Videoconferencing to validate the identity of the holders;
- Creation or update of entities requesting certification services;
- Validation of the documentation to be submitted by the holder for certificates issuance / revocation;
- Validation of the identity of the holders by videoconference;
- Notification to holders, when necessary:
- Safeguard of artefacts under its custody.

e) Audit Working Group (Auditor)

Responsible for the internal analysis, in accordance with national and European rules applicable to the activities of GTS, in its capacity of a qualified trust service provider, being authorized to check and monitor activities archives of trust systems. This group has the following responsibilities:

- Registration and monitoring of all sensitive system operations;
- Registration of all procedures subject of being audited;
- Periodic verification of the conformity with processes, policies and procedures in force within the context of the activity of a qualified service provider;
- Safeguard of artefacts under its custody;
- Submission of proposals for improvement.

f) Management Working Group (Management)

Responsible for assuring technical, financial and personnel means, for the adequate functioning of GTS, in its capacity of a qualified trust service provider. This group has the following responsibilities:

- Appointment of members of the other Working Groups;
- Review and approval of GTS Policies and Practice Statements;
- Safeguard of artefacts under its custody.

5.2.2. Number of Individuals Required per Task

Each group have 2 members to ensure the redundancy of resources.

5.2.3. Identification and Authentication for each Role

See section 5.2.1.

5.2.4. Roles Requiring Separation of Duties

The composition of the working groups must respect the principles of minimum privilege and segregation of functions. The following table shows the incompatibilities between the different groups existing in GTS, in order to avoid any conflicts of interest.

Working Group	Incompatible with				
	(a)	(b)	(c)	(d)	(e)
(a) Security Administration		X	X	X	X
(b) System Administration	X				X
(c) Registry Administration	X				X
(d) Systems Operation	X				X
(e) Audit	X	X	X	X	

5.3. Personnel Controls

5.3.1. Qualifications, Experience and Clearance Requirements

All members included in any GTS working groups should meet the following requirements:

- Proof of qualification and experience for the performance of the respective duty;
- Ensure confidentiality related to GTS sensitive information or identification data of holders;
- Guarantee that they do not perform functions that may arise a conflict with their responsibilities concerning GTS activities;
- Ensure knowledge of the terms and conditions for the performance of the respective function;
- Have the necessary documentation for the performance of the respective function;
- Have been formally appointed for the function to be exercised.

5.3.2. Background Check Procedures

Background check is derived from the process of accreditation of persons appointed to pursue activities in any of the Working Groups and that includes the verification of identity and criminal record, as well as references mentioned in the curriculum vitae.

5.3.3. Training Requirements and Procedures

The members of the Working Groups must be subject to a specific training and education plan, which covers the following topics:

- Legal aspects related to certification services;

- Digital certificate and public key infrastructure;
- General concepts on information security;
- Specific training for the related Working Group;
- GTS software and/or hardware operation;
- Certification Policies and Certification Practice Statements;
- Awareness on evaluation criteria for SSL certificates according to the CA/Forum Browser EV Guidelines;
- Procedures for continuity of the activity;
- Recovery in case of disasters.

5.3.4. Retraining Frequency and Requirements

The occurrence of any technological change, or the introduction of new tools, or the modification of existing procedures, should trigger an adequate training process in all Working Groups. In addition, training sessions should be addressed to members of Certification Authorities when GTS Certificate Policies or Certification Practice Statement are amended. Such facts must be taken into account in order to guarantee the intended level of knowledge for the successful implementation of responsibilities incumbent to the different Working Groups.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

All unauthorized actions and those actions violating GTS Certification Practice Statement and Certificate Policies shall be subject to disciplinary measures, either that they have been deliberate or caused by negligence. In addition, and depending on the seriousness of the infringement, legal sanctions may be applied.

5.3.7. Independent Contractor Controls

The access to the High Security Zone by consultants or providers of independent services, requires the continuous supervision from members of the Working Groups, being their identity confirmed through the verification of documentation issued by reliable sources. In addition, they must register in the book of attendance existing for this purpose.

5.3.8. Documentation Supplied to Personnel

Information and documentation related to GTS Certificate Policies, GTS Certification Practice Statement, documentation with description of responsibilities, duties and tasks depending on the function, as well as additional technical documentation about the software and hardware used by the GTS Certification Authority, must be available to Working Groups members.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

All significant events, able to be auditable, should be recorded, in particular the following:

- Security backups, restoration or data file;
- Physical security of input/output of the different levels of security devices;
- System maintenance;
- Software and hardware modifications and updates;
- Change of personnel;
- Connect and disconnect applications or systems involved in the certification activity;
- Operations conducted by members of the Working Groups;
- Attempts, successful or not, to access sensitive resources of GTS Certification Authority;
- Attempts, successful or not, to modify security parameters;
- Attempts, successful or not, to create, modify, or delete system accounts;
- Attempts, successful or not, to start and end of session;
- Attempts, successful or not, of transactions related to the request, issuance, renewal, modification, suspension and revocation of certificates and keys;
- Attempts, successful or not, to generate, issue or update the CRL;
- Attempts, successful or not, to create, modify or delete information of certificates holders;
- Attempts, successful or not, to access GTS TSA High Security Zones.

The record of events, by automatic or manual means, must contain, at least, information such as event date and time, category, description and serial number, as well as the identification of the agent that caused them.

5.4.2. Frequency of Processing Audit Log

The audit of records shall be conducted on a regular basis, in particular on the occurrence of events which may be considered suspicious or which may compromise in any way the activity in question. All such events should be recorded in an analysable summary report, as well as the decisions and actions taken in response.

5.4.3. Retention Period for Audit Log

Audit records must be kept in the system for at least 1 month after being processed. After that time, they must be filed according to as is defined in section 5.5 of this document.

5.4.4. Protection of Audit Log

Audit records are protected against unauthorized access, amendments, manipulation or destruction attempts. As a rule, electronic records must be protected using cryptographic techniques so nobody, except the own records visualization applications, with appropriate access control, can access them. Manual records are stored in premises which meet the requirements defined for that purpose, within the GTS TSA safe facilities. This type of audit records is considered as sensitive information.

5.4.5. Audit Log Backup Procedures

Backups of audit logs are made on a regular basis.

5.4.6. Audit Log Accumulation System (Internal vs. External)

Logs are centrally collected and processed.

5.4.7. Notification to Event-Causing Subject

Events likely to be audit are recorded in GTS internal systems, being stored in a secure manner. It is not envisaged any notification to the event-causing subject.

5.4.8. Vulnerability Assessment

Although significant changes in the GTS TSA global environment are not yet produced, vulnerability assessments must be conducted, with the aim to minimize or eliminate potential attempts of security breaches in the system. The outcome of these evaluations should be informed to the responsible managers so they can review and approve, when required, an implementation plan and the correction of detected vulnerabilities.

5.5. Records Archival

5.5.1. Types of Records Archived

The GTS TSA shall archive, at minimum, the following types of data:

- Audit records specified in this document;

- Security copies of systems that are part of the CA infrastructure;
- Documentation related to certificates life cycle;
- Keys for confidentiality purposes (where applicable);
- Contracts celebrated between the CA and other entities.

5.5.2. Retention Period for Archive

The retention time of data subject to archiving is defined in accordance with the provisions of national legislation, for a period of no less than 7 years.

5.5.3. Protection of Archive

The archive is protected according to what is also foreseen for the protection of audit records. Furthermore, the archive is protected so that only authorised members of the Working Groups may consult and access it.

5.5.4. Archive Backup Procedures

See section 5.4.5.

5.5.5. Requirements for Time-Stamping of Records

Information systems used by the GTS TSA must ensure the record of the date and time of the moment, based on a secure time source.

5.5.6. Archive Collection System (Internal or External)

See section 5.4.6.

5.5.7. Procedures to Obtain and Verify Archive Information

Only duly authorised members of the Working Groups have access to the archives for the purpose of checking the integrity of the information to ensure that it is in good condition and can be recovered.

5.6. Key Changeover

No stipulation.

5.7. Compromise and Disaster Recovery

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

5.7.1. Incident and Compromise Handling Procedures

In case of a serious security incident or compromise of the GTS TSA, the following procedures shall be performed:

- Notification without undue delay, but always within a period of 24 hours after detecting the event, to the supervisory authority and, if necessary, to other entities, such as the competent national body on information security or the authority responsible for data protection, of all the breaches of security or loss of integrity that have a significant impact on the trust service provided or on stored personal data.
- If the security breach of loss of integrity is likely to harm the natural or legal person to whom the trust service is provided, that person will be notified, without undue delay, about the above-mentioned security breach or loss of integrity.
- In addition, and depending on the type of incident, the affected CA may be disconnected.

If necessary, if the security breach or integrity loss affect two or more Member States, the notified supervisory authority shall inform about this fact to supervisory authorities of the other Member States concerned and to ENISA.
The notified supervisory authority shall inform to the public, or will demand the trust service provider to do so, if considers that the disclosure of the security breach or loss of integrity is of public interest.

5.7.2. Recovery Procedures if Computing resources, software, and/or data are corrupted

When hardware, software, and/or data resources have been altered or there is suspicion that these have been corrupted, an event management procedure will be activated to restore secure conditions adding new credible efficiency components. GTS will suspend its services and will notify all entities involved in case it is verified that this situation has affected issued certificates, including notification to the holders thereof.

5.7.3. Recovery Procedures after Key Compromise

If any of the algorithms, or associated parameters, used by the GTS TSA or its owners become insufficient for their intended purpose, the GTS TSA shall:

- Inform all holders and other entities with which the GTS TSA has agreements or other form of established relationships. Additionally, this information shall be made available for other dependent entities;
- Inform the Mozilla Root Repository and other root repositories that have established a trust relationship with the GTS PKI hierarchy;
- Schedule the revocation of any affected certificate.

5.7.4. Business Continuity Capabilities after a Disaster

GTS has a business continuity plan, which describes all the procedures to be implemented in the event of a disaster where there is loss or corruption of data, software and equipment. The Continuity Plan should ensure that services identified as critical due to their availability necessity are accessible at the Alternative Location and that GTS TSA data necessary to resume operations is copied and stored in safe and adequate locations to allow the proper return to operations of GTS TSA in case of incidents/disasters. Backup copies of essential information and software are performed regularly. Adequate support facilities must be provided to ensure that essential information and software can be recovered after a disaster or failure in the media. Safeguard mechanisms must be tested regularly to ensure that they meet the requirements of the plans for business continuity.

5.8. CA or RA Termination

In the event of termination of activities, GTS should proceed promptly to the following actions:

- Inform the Supervisory Authority (National Security Department -*Gabinete Nacional de Segurança* - GNS);
- Inform all holders of certificates through a notification explaining in advance the cessation of formal activities of GTS TSA;
- Revocation of all certificates;
- Ensure the transfer (for its retention by another organization) of all information concerning the CA activity, in particular, CA key, certificates, documents in files (internal or external), repositories and events records files;
- Proceed to the complete destruction of all classified information or ensure its transfer (for permanent retention by another organization) of all information regarding GTS TSA, activity, in particular, CA key, certificates, documents in files (internal or external), repositories, and events records files.

In case of changes in the responsible body/structure for managing the GTS TSA activity, the GTS TSA shall inform the entities listed in the previous paragraphs of such fact.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

This section defines the security measures implemented for the GTS PKI in order to protect the cryptographic keys generated by it, and respective activation data. The security level assigned for key maintenance shall be maximum so that private keys and secure keys, as well as activation data, are always protected and only accessed by duly authorised persons. The generation of key pairs of the GTS TSA is processed in accordance with the requisites and algorithms defined in this policy.

6.1.1. Key Pair Generation

The generation of key pairs of the GTS ROOT CA is processed in accordance with the requisites and algorithms defined in this statement, through a formal procedure dated, carried out, and signed by authorised members of the Security Administration and Audit Working Groups. The GTS CA does not generate key pairs for certificates that have the EKU extension containing the ***KeyPurposeIds***, ***id-kp-serverAuth*** or ***anyExtendedKeyusage*** attributes.

6.1.1.1. CA Key Pair Generation

The generation of key pairs of the GTS TSA is processed in accordance with the requisites and algorithms defined in this statement, through a formal procedure dated, carried out, and signed by authorised members of the Security Administration and Audit Working Groups. The GTS TSA does not generate key pairs for certificates that have the EKU extension containing the ***KeyPurposeIds***, ***id-kp-serverAuth*** or ***anyExtendedKeyusage*** attributes.

6.1.1.2. RA Key Pair Generation

No stipulation.

6.1.1.3. Subscriber Key Pair Generation

See section 4.5.1.

6.1.2. Private Key Delivery to Subscriber

No stipulation.

6.1.3. Public Key Delivery to Certificate Issuer

See section 4.1.

6.1.4. CA Public Key Delivery to Relying Parties

See section 2.2.

6.1.5. Key Sizes

Concerning the size of the keys, the recommendations of the ETSI TS 119 312 - Electronic Signatures and Infrastructures - Cryptographic Suites standard were followed. The size defined for the keys is the following:

- 4096 bits RSA for the key of the GTS Certifying Authorities;
- 2048 bits RSA for keys associated with the remaining certificates that are issued by GTS with the sha256RSA signature algorithm.

6.1.6. Public Key Parameters Generation and Quality Checking

The key generation process is, necessarily, carried out directly in a cryptographic module in hardware (HSM). The cryptographic module complies with the FIPS 140-2 level 3 requisites. These certificates are signed by the GTS ROOT CA. The GTS ROOT CA works in offline mode.
The generation of the GTS TSA keys shall be carried out in accordance with that stipulated in PKCS#11.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

See section 1.4.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

This section addresses the requirements for the protection of the private keys and for the cryptographic modules of the GTS PKI. Global Trusted Sign has implemented a combination of physical, logical and procedural controls, duly documented, in order to ensure the confidentiality and integrity of the private keys of the GTS PKI.

6.2.1. Cryptographic Module Standards and Controls

The GTS TSA uses cryptographic modules (HSM) for activities related to the generation, storage and signature. Cryptographic modules are compliant with Common Criteria v2.3, FIPS 140-2 level 3 (for GTS ROOT CA cryptographic module). The GTS TSA cryptographic module security is guaranteed during its life cycle, ensuring the following:

- The installation and activation of keys in the cryptographic module is conducted by members of the Working Groups duly identified (section 14.2, Processes Controls, and section 14.3, Staff Security Measures);
- Private signature keys stored in the cryptographic module are deleted at the end of their life cycle;
- The cryptographic module was not tampered with during its transport;
- The cryptographic module is not tampered with while remaining at GTS secure premises;
- The cryptographic module has proper operation.

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

The generation and installation of the activation data for the private key of the GTS TSA is carried out by authorised personnel in a safe environment through an initial setup of the HSM, which requires simultaneous control by two members of the working groups.

6.2.3. Private Key Escrow

The GTS TSA retains its private key and the private keys of all its customers through an HSM kept in a safe environment.

- Are internally archived in a safe environment and for long periods of time;
- Are generated and stored in the HSM, being unable to be transferred to other media or devices;
- The GTS TSA private keys have, at least, a backup copy with the same level of security than the original key and they are subject of backups;
- Are stored in encrypted form in the HSM.

6.2.4. Private Key Backup

Refer to previous point.

6.2.5. Private Key Archival

See section 6.2.3.

6.2.6. Private Key Transfer into or from a Cryptographic Module

The transmission of the activation data of the private keys to other HSM is made, only and exclusively when necessary, in order to guarantee its protection and availability.

6.2.7. Private Key Storage on Cryptographic Module

See section 6.2.3.

6.2.8. Activating Private Keys

The private key must be activated when the ROOT CA system/application is connected. This activation must be performed only when, previously, the authentication in the cryptographic module is made by the persons indicated for this purpose, being mandatory the use of authentication by quorum *k* in *N*, where *k* = 2. That means, it is necessary *k* users in *N* to make an administrative operation in the HSMs (including the activation of the private key).

6.2.9. Deactivating Private Keys

The private key must be deactivated when the ROOT CA system/application is disconnected. This deactivation must only be performed when, previously, the authentication has been made in the cryptographic module by the persons indicated for this purpose, being mandatory the use of authentication by quorum k in N, where k = 2. That means, it is necessary k users in N to make an administrative operation in the HSMs (including the deactivation of the private key).

6.2.10. Destroying Private Keys

The GTS TSA different keys shall be destroyed when they are no longer necessary. Usually, keys destruction must be always preceded by the certificate revocation, in the case of still being valid, or in case that it has reached the end of their date of validity. Accordingly, keys must be deleted/destroyed by an auditable formal method, to avoid their reconstruction. Also, respective backup copies must be subject to destruction.

6.2.11. Cryptographic Module Capabilities

See section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The GTS TSA archives its keys, and those keys issued by it (for digital signatures purposes), remaining stored after the expiry of corresponding certificates for verification of digital signatures generated during its validity period.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The period to use the keys is determined by the validity period of the certificate, so that after the certificate expires, the keys can no longer be used, originating the permanent termination of their operability and of the use for which they were meant. The validity of the various types of certificates and the period in which they should be renewed is as follows:

- The GTS ROOT CA certificate has a minimum validity of 20 years;
- A subordinate entity certificate issued by the GTS TSA has a minimum validity of 1 year, and a maximum validity of 6 years;

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

See section 6.2.2.

6.4.2. Activation Data Protection

The private key activation data is stored in safe environments.

6.4.3. Other Aspects of Activation Data

Activation data is destroyed once the associated private key has been also destroyed.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Access to the GTS PKI servers is restricted to the members of the Working Groups. The GTS ROOT CA is an offline CA, only activated within the scope of periodic maintenance and deactivated immediately afterwards. The Subordinate CAs of the GTS PKI have an active operation, and the request for issuing certificates is made from the Certificate Life Cycle Management System (CLCMS) and/or from the operation console.

6.5.2. Computer Security Rating

The various systems and products used by the GTS PKI are reliable and protected against modification. The cryptographic modules comply with Common Criteria v2.3, FIPS 140-2 and FIPS 140-2 level 3 for the GTS ROOT CA cryptographic module.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

All development, settings, and modifications on the software/hardware associated with the public key infrastructure are implemented and audited by authorized members of the GTS TSA. The GTS TSA has mechanisms to control and monitor the GTS TSA system settings, from its initial activation until eventual termination of activities. All upgrade and maintenance operations are carried out by authorised members in accordance with the appropriate procedures.

6.6.2. Security Management Controls

All GTS TSA systems are in the High Security Zone (HSZ). Through the implemented controls, it is possible to guarantee the identification, authentication and administration of accesses.

6.6.3. Life Cycle Security Controls

The upgrade and maintenance operations of the GTS PKI products and systems, follow the same control as the original equipment and are installed by members of the GTS Trust Groups with adequate training for the purpose, following the defined procedures.

6.7. Network Security Controls

The GTS PKI has border protection devices, namely a firewall system. It meets the necessary requirements for identification, authentication, access control, administration, auditing and information exchange. Therefore, the PKI GTS ensures that the set of controls implemented are in conformity with all the network security requirements of the “CA/Browser FORUM - Network and Certificate System Security Requirements”.

6.8. Time-Stamping

Information related to the GTS TSA is registered with the date and time of creation. All the infrastructure is time-synchronized through internal atomic clock, and by two alternative UTC sources:

- Royal Observatory of Belgium (ORB), Brussels, Belgium - ntp1.oma.be
- Observatoire de Paris (LNE-SYRTE), Paris, France - ntp-p1.obspm.fr

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

The Timestamp certificate profile complies with ETSI 319 412 and ETSI 319 422 standards.

a) Profile of the Timestamping Authority Certificate

OID	Componente do Certificado	Valor	Tipo	Comentários
	Version	V3	M	
	Serial Number	<Assigned by the CA to each certificate>	M	
1.2.840.113549.1.1.11	**Signature**	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Certificate's signature. The value must be equal to the OID of the *SignatureAlgorithm* (below)
	Issuer		M	
	Country (C)	"PT"		Country of the issuing authority
	Organization (O)	"ACIN iCloud Solutions, Lda"		Name of the organization of the issuing authority
	Organization Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	Global Trusted Sign Certification Authority 01		
	Validity			Validity of the Certificate
	Valid from	<Date of issuance>		14-07-2022
	Valid to	<Date of issuance + 8 years>		8-year maximum validity
	Subject		M	
	Country (C)	PT		Nationality of the certificate's holder
	Organization (O)	ACIN iCloud Solutions, Lda		
	Organization Unit (OU)	Global Trusted Sign		
	Common Name (CN)	Global Trusted Sign Timestamping Authority 002		
	Subject Public Key Info		M	
1.2.840.113549.1.1.1	Algorithm	rsaEncryption (OID: 1.2.840.113549.1.1.1)		Public key algorithm
	subjectPublicKey	<Public Key>		Certificate public key
	Authority Key Identifier		M	
	keyIdentifier	160-bit hash		It allows to identify the public key corresponding to the private key of the certificate
	Subject Key Identifier	160-bit hash	M	Certificate key identifier
	Key Usage		M	

OID	Componente do Certificado	Valor	Tipo	Comentários
	Digital Signature	"1" selected		
	Non-Repudiation	"1" selected		
	Key Encipherment	"0" selected		
	Data Encipherment	"0" selected		
	Key Agreement	"0" selected		
	Key Certificate Signature	"0" selected		
	CRL Signature	"0" selected		
	Encipher Only	"0" selected		
	Decipher Only	"0" selected		
1.3.6.1.5.5.7.3.8	**Enhanced Key Usage**	Time Stamping (1.3.6.1.5.5.7.3.8)		
	Certificate Policies		M	
1.3.6.1.4.1.50302.1.1.1.3.1.0	[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.1.3.1.0 Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identifier and location of the GTS TSA Certification Practice Statement
1.3.6.1.4.1.50302.1.1.2.3.1.0	[2]	BST policy-identifier: 0.4.0.2023.1.1 Own policyIdentifier: 1.3.6.1.4.1.50302.1.1.2.3.1.0 cPSuri: https://pki.globaltrustedsign.com/index.html		best-practices-ts-policy Identifier and location of the Timestamp Certificate Policy
	Basic Constraints		M	
	Subject Type	End Entity	C	Certificate intended for Timestamping
	PathLenConstraint	None		
	CRLDistributionPoints		M	
	[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_subca_crl.crl		Location of the GTS SUBCA Certification Revocation List
	[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_subca_crl.crl		Secondary location of the GTS SUBCA Certification Revocation List
1.2.840.113549.1.1.11	**Signature Algorithm**	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Algorithm used to create the signature of the certificate

OID	Componente do Certificado	Valor	Tipo	Comentários
	Signature Value	<It contains the digital signature issued by the CA>	M	Signature of the certificate

7.1.1. Version Number(s)

The ***version*** field of the certificate describes the version used in encoding the certificate. In this profile, the version used is 3 (V3).

7.1.2. Certificate Content and Extensions; Application of RFC 5280

The components and extensions defined for X.509 v3 certificates provide methods to associate attributes to users or public keys, as well as to manage the certification hierarchy

7.1.2.1. Root CA Certificate

Information is available in the certificates on file, which may be consulted by accessing the https://pki.globaltrustedsign.com/ repository and in document PL11 – GTS ROOT Certificate Policy.

7.1.2.2. Subordinate CA Certificate

See section 7.1.2.1.

7.1.2.3. Subscriber Certificate

See section 7.1.2.1.

7.1.2.4. All Certificates

Information is available in the certificates on file, which can be consulted by accessing the https://pki.globaltrustedsign.com/index.html repository and through PL01_GTS - Qualified Signature Certificate Policy; PL02_GTS - Electronic Seals Certificate Policy; PL03_GTS -EV SSL Certificate Policy; PL04_GTS – OV SSL Certificate Policy; PL16_GTS - Advanced Signature Certificate Policy; PL17_GTS - Advanced Electronic Seal Certificate Policy; and PL14_GTS - Timestamp Certificate Policy.

7.1.2.5. Application of RFC 5280

The components and extensions defined for X.509 v3 certificates provide methods to associate attributes to users or public keys, as well as to manage the certification hierarchy.

7.1.3. Algorithm Object Identifiers

7.1.3.1. SubjectPublicKeyInfo

Information is accessible in the profiles of the certificate, section 7.1.

7.1.3.2. Signature AlgorithmIdentifier

The certificate ***signatureAlgorithm*** field contains the OID of the cryptographic algorithm used by the GTS CA to sign the certificate (1.2.840.113549.1.1.11 - sha256WithRSAEncryption).

7.1.4. Name Forms

7.1.4.1. Name Encoding

See section 3.1.

7.1.4.2. Subject Information - Subscriber Certificates

See section 3.1.

7.1.4.3. Subject Information - Root Certificates and Subordinate CA Certificates

See section 3.1.

7.1.5. Name Constraints

In order to ensure total interoperability between applications that use digital certificates, it is recommended to use only alphanumeric characters without accents, space, underline, minus symbol and full stop ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') on X.500 directory entries.

7.1.6. Certificate Policy Object Identifier

All certificates issued by the GTS PKI contain the following qualifiers: "*policyQualifIierID*= CPS" and "*cPSurl*", which points to the URL where the Certification Practices Statement with the OID identified by the "*policyIdentifier*" is found.

7.1.6.1. Reserved Certificate Policy Identifiers

See section 7.1.6.1.

7.1.6.2. Root CA Certificates

See section 7.1.6.1.

7.1.6.3. Subordinate CA Certificates

See section 7.1.6.1.

7.1.6.4. Subscriber Certificates

See section 7.1.6.1.

7.1.7. Usage of Policy Constraints Extensions

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

The "*certificate policies*" extension contains a type of policy qualifier to be used by certificate issuers and certificate policy authors. The type of qualifier is "*CPSuri*", which contains a pointer, in the form of URL, to the Certification Practices Statement published by the CA and the "*userNotice explicitText*", which contains a pointer, in the form of URL, to the Certificate Policy.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

7.2.1. Version Number(s)

The issued CRLs contain the basic fields and contents, which are detailed in the following table:

Field	Value
Version	V2
Signature Algorithm	The algorithm used by the CA to sign the certificate is sha256WithRSAEncryption
Issuer	DN of the certification authority issuer of the CRL
Effective date	Indication of when the CRL was generated
Next update	Indication of when a new CRL will be generated
Revoked Certificates	Certificate revocation list that provides information on the status of the certificates regarding serial number of the revoked certificate, date when it was revoked and the reason for its revocation

More detailed information on the CRL and OCSP profiles can be found at:

- GTS CA Certificate Revocation List (CRL)
  https://pki.globaltrustedsign.com/index.html

- GTS CA Certificate Revocation List (CRL)
  https://pki02.globaltrustedsign.com/index.html

OCSP Certificates profiles can be consulted at:

- http://ocsp.globaltrustedsign.com

7.2.2. CRL and CRL Entry Extensions

Extension	Value
Authority Key Identifier	Identifier of the CA issuing the CRL
CRL Number	Sequential number of the CRL

7.3. OCSP Profile

7.3.1. Version Number(s)

OCSP requests and responses issued by the GTS PKI comply with RFC 6960, version 1.

7.3.2. OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessments

GTS shall perform regular audits and conformity assessments to ensure the conformity of Certification Authorities which are part of its trust hierarchy in accordance with the applicable national legislation, as well as international standards.

8.1. Frequency or Circumstances of Assessment

Conformity audits in the GTS TSA will be conducted regularly in accordance with the applicable legislation by an external entity registered and recognized for that purpose, on the basis of existing standards, and results will be communicated to the supervisory authority.

8.2. Identity/Qualifications of Assessor

The Conformity Assessment Body (CAB) is the body defined in number 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited under that Regulation as being competent to carry out conformity assessment of qualified trust service providers and the trust services they provide.

8.3. Assessor´s Relationship to Assessed Entity

The conformity assessment body and its team members are independent, not acting either partially or discriminatory in relation to the entity that is subject to audit. On the relationship between the Auditor and the entity subject to audit, it must be assured the absence of any contractual link. The Auditor and the audited party (Certification Authority) must not have any relationship, current or expected, financial, legal or any other which may lead to a conflict of interest. The Auditor must take into consideration the compliance with the provisions of the legislation in force of aspects related to personal data protection, to the extent allowed to the auditor to access personal data contained in the GTS TSA holders' files.

8.4. Topics Covered by Assessment

A security audit is conducted on the basis of the requirements defined in this CP and in accordance with applicable national legislation. It aims to determine the conformity of the GTS TSA services defined in this Certificate Policy. Also, it must determine the proper adequacy in relation to several documents, particularly with policies related to security, physical security, technology assessment, TSA services management, selection of staff, certification practice statements and policies of valid certificates, contracts and privacy policies. It can be general or partial, and it can have incidence on any type of documents/processes.

8.5. Actions Taken as a Result of Deficiency

When irregularities are detected in an audit, the CAB shall:

- Document all the deficiencies found during the audit;
- At the end of the audit process, meet with the persons responsible of the authority under audit and submit a brief first impressions report (FIR);
- Prepare the audit report in accordance with the rules and practices established by the Supervisory Authority;
- Submit the audit report to the audited Authority;
- The entity under audit must send an irregularities correction report (ICR) to the Supervisory Authority, describing actions, methodology and time required for the correction of identified deficiencies;
- After the analysis of the report submitted, and depending on the level of seriousness/severity of irregularities, the Supervisory Authority shall select one of the following three options:
    - Accept the terms, allowing business continuity until the next inspection;
    - Allow authority business continuity for a maximum period of 90 days for the correction of irregularities;
    - Immediate revocation of activities.

8.6. Communication of Results

Results of the whole process shall be communicated to the responsible auditors and to GTS.

8.7. Self-Audits

During the period in which the GTS TSA issues certificates, it monitors, therefore, the subscription to the Certificate Policies and Certification Practices Statements, thus controlling all requisites for qualitative assurance of service through internal audits carried out quarterly, through a randomly selected sample of at least three percent of the certificates issued during the period to which the audit refers. This audit is carried out by members of the GTS Trust Group, according to the guidelines adopted by the CA/B FORUM.

9. Other Business and Legal Matters

It is important to highlight some legal and commercial aspects:

- Fees derived from certificates issuance and/or renewal procedures may be charged;
- Fees derived from chronological validation services may be charged;
- Fees by the availability of certificates in repository will not be charged;

- Access to information about the status or the revoked certificates list (CRL) is free, and no fee is applicable;
- No refunds for the provision of certificate revocation services are applicable.

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

The fees charged by GTS are indicated at https://globaltrustedsign.com/ or in a formal proposal made by GTS.

9.1.2. Certificate Access Fees

No stipulation.

9.1.3. Revocation or Status Information Access Fees

Access to information on the certificate or revocation status (CRL) is free of charge.

9.1.4. Fees for Other Services

Fees for other services are identified in a formal proposal.

9.1.5. Refund Policy

The GTS TSA does not have a specific refund policy.
The correct issuance of a digital certificate, of any kind, implies the start of the execution of a contract, therefore, in accordance with the legislation applicable to consumer protection, in these cases, the Subscriber loses the right of termination, and consequently, of reimbursement.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Certification Authorities must respect the legislation in force regarding insurance coverage for civil liability. In this sense, GTS has civil liability insurance, in accordance with article 16 of Decree-Law 62/2003, of 3 April.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

GTS has a civil liability insurance, in accordance with article 16 of Decree-Law 62/2003, of 3 April.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following is considered as confidential information:

- Certification Authorities private keys;
- Certificate holders' private keys;
- All information concerning parameters of security, control and audit procedures;
- All personal information supplied to GTS TSA during the registration process of certificate subscribers, unless there is an explicit authorization for its disclosure;
- Business continuity and recovery plans;
- Transactions records, including complete records and audit records of transactions;
- GTS TSA working groups members data.

9.3.2. Information not Within the Scope of Confidential Information

The following is considered as public access information:

- Certification Practice Statements;
- Certification Policies;
- Certificate Revocation Lists (CRLs);
- All information classified as "public".

The GTS TSA allows access to non-confidential information, without prejudice to that which shall be established in the CP, in the domain of security controls necessary to protect its authenticity and integrity.

9.3.3. Responsibility to Protect Confidential Information

The GTS TSA practices ensure the protection of confidentiality and integrity of the registration data, especially when transmitted between the GTS TSA and the subscribers and holders, as well as during the communication between the distributed components of the GTS TSA systems. Within the scope of the services provided, it is necessary to maintain digital evidence for compliance matters with the legislation in force and applicable to the GTS TSA. These evidences are kept in order to guarantee their safe collection, transmission, and storage.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

The Certificate Life Cycle Management System (CLCMS) is responsible for implementing measures that ensure the privacy of personal data, in accordance with applicable Portuguese and European legislation.

9.4.2. Information Treated as Private

Private information is any information supplied by the holder of the certificate that is not publicly available.

9.4.3. Information not Deemed Private

Non-private information is information made public from certificates and therefore is not considered private.

9.4.4. Responsibility to Protect Private Information

Responsibility for the protection of private information is in accordance with the Portuguese legislation, particularly with the General Data Protection Regulation (Regulation 2016/679).

9.4.5. Notice and Consent to Use Private Information

Procedures for notification and consent to use private information are in accordance with Portuguese law, in particular with the General Data Protection Regulation (Regulation 2016/679).

9.4.6. Disclosure Pursuant Judicial or Administrative Process

There is no transfer of personal data to third parties, except for duly substantiated legal reasons

9.4.7. Other Information Disclosure Circumstances

There is no transfer of personal data to third parties, except for duly substantiated legal reasons

9.5. Intellectual Property Rights

All intellectual property rights, including those referred to issued certificates and CRL, OID, CPS, CP, as well as any other related documents, are property of GTS. The private keys and the public keys are

property of the holder, independent of the physical means used for storage. The holder always retains the right to his/her trademarks, products or commercial name contained in the certificate.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

The GTS TSA is obliged to comply with the following directives:

- To conduct its operations in accordance with this Policy and respective Certificate Practice Statement;
- To clearly state all its Certification Practices in the appropriate document;
- To comply with specifications defined in the law on Personal Data Protection;
- To protect, where they exist, their private keys and those under its custody;
- To issue certificates in accordance with standard X.509;
- To issue certificates in accordance with the information known at the time of its issuance and free of data input errors;
- To ensure confidentiality during the process of generation of data provided for the creation of signature and its delivery to its holder through a safe procedure;
- To use reliable products and systems that are protected against any alteration and which ensure the technical and cryptographic security of the certification procedures;
- To use reliable systems to store recognized certificates, enabling to verify its authenticity and to prevent unauthorised data alteration;
- To archive, without amendments, issued certificates;
- To ensure that it can be determined, with accuracy of date and time, that a certificate has been issued, or revoked, or suspended;
- To employ staff with skills, knowledge and experience required for the provision of certification services;
- To revoke certificates under the terms provided in the present document, and to update the revoked certificates list in the CRL, with the frequency stipulated in this CP;
- To publish its CPS and applicable policies in its repository guaranteeing the access to current and previous versions;
- To notify certificate holders by email, and without delay, when GTS TSA proceeds to their revocation or suspension, indicating the reason that caused the situation;
- To collaborate with external audits required by the Supervisory Authority;
- To operate in accordance with the policies, standards and regulations that may apply;
- To ensure the availability of the CRL in accordance with provisions set in this document, as well as the availability of the OCSP service;

- To notify the Supervisory Body, at least three months in advance, in the event of cessation of activities, as well as to all holders of certificates issued by the GTS TSA;
- To preserve all information and documentation concerning a qualified certificate and the Certification Practice Statements in force at any time during the period set out in the present document;
- To provide the GTS TSA certificates.

9.6.2. RA Representations and Warranties

Global Trusted Sign Registration Authorities meet the requirements set forth in this document and are subject to independent External Audits, as well as Internal Audits performed by Global Trusted Sign on a regular basis.

a) Internal Registration Authority

Within the scope of the Global Trusted Sign Certification Authority, the registration authority is executed by its internal services, which have the responsibility of validating the necessary data, as explained in the specific Global Trusted Sign Policies, for each one of the services provided.

b) External Registration Authority

Global Trusted Sign has no External Registration Authorities.

9.6.3. Subscriber Representations and Warranties

Holders of issued certificates are obliged to comply with the following directives:

- To limit and to adapt the use of certificates in accordance with the legislation in force and with the uses established in this document;
- To adopt all care and measures necessary to ensure the possession of their private key;
- To immediately request the revocation of a certificate, when there is knowledge or suspicion of compromise of the private key associated to the public key contained in the certificate, in accordance with the procedures specified herein;
- Not to use a digital certificate that has lost its effectiveness, either by having been revoked, suspended or by having expired its validity period;
- To submit to Certification Authorities (or Registration Entities) information deemed accurate and complete in relation to the data requested to conduct the registration process. CA must be notified of any change of such information;

- Not to monitor, manipulate or perform actions of "reverse engineering" on the technical implementation (hardware and software) of certification services, without the GTS TSA prior authorization, in writing.

9.6.4. Relying Party Representations and Warranties

Parties relying on the certificates issued by the GTS TSA are obliged:

- To limit the reliability of the certificates to the uses allowed for them in conformity with the legislation in force and with the present document;
- To verify certificates validity during any operation based on them;
- To assume responsibility for the duly verification of digital signatures;
- To assume responsibility for the verification of the validity, revocation or suspension of trusted certificates;
- To assume responsibility for the proper verification of issued certificates;
- To have full knowledge of the guarantees and responsibilities applicable to the acceptance and use of trusted certificates and to agree to be bound to them;
- To notify any anomalous fact or situation concerning the certificates, by using means published by the GTS TSA in its website.

9.6.5. Representations and Warranties of other Participants

No stipulation.

9.7. Disclaimer of Warranties

The GTS TSA disclaims all warranties of service which are not related in the obligations set out in this CP.

9.8. Limitations of Liability

The GTS TSA is liable for any damages caused to end users and relying parties that may arise from its activity, in accordance with the applicable legislation. The GTS TSA is not responsible for any loss or damage derived from abusive use or beyond the scope of the contract established with users and/or relying parties. The GTS TSA does not assume any responsibility in the event of services failure related to force majeure, such as natural disasters, war or other similar.

9.9. Indemnities

The GTS TSA will assume responsibility regarding any compensation, in accordance with the applicable legislation in force.

9.10. Term and Termination

9.10.1. Term

This CP comes into force from the moment of its publication at the GTS TSA repository and after its approval, on the terms of this document. This CP will be in effect while not revoked expressly by a new version issuance, under the terms of this document, or by the renewal of the GTS TSA keys, when, mandatorily, a new version shall be written.

9.10.2. Termination

This CP will be replaced by a new version, regardless of the significance of the changes made to it, so that it will always be of full implementation. When the CP is revoked, it will be removed from the public repository, however, it is ensured that it will be preserved during the period defined in the present document.

9.10.3. Effect of Termination and Survival

Obligations and restrictions defined in this CP, related to audits, confidential information, obligations and responsibilities of the GTS TSA, that emanate from its entry into force, will preserve after its replacement or revocation, by a new version, in all that is not contrary to this one.

9.11. Individual Notices and Communications with Participants

All participants must use appropriate mechanisms for collective communication, including digitally signed e-mails, postal mail and signed forms, among others, using the most suitable according to the nature of each case.

9.12. Amendments

9.12.1. Procedure for Amendment

Amendments to this CP must be approved by the Management Group. Amendments must be carried out through documents, containing the new amendments to the CP.

9.12.2. Notification mechanism and period

In the case in which the Management Group considers that the amendments to the specification may affect the acceptability of the certificates for specific purposes, it shall be communicated to the users of the corresponding certificates that an amendment was made and that they should consult the new CP in the repository established. The communication mechanism shall be the website https://www.globaltrustedsign.com.

9.12.3. Circumstances under which OID must be Changed

If the GTS TSA determines that a change to the identifier (OID) of the certificate policy (CP) is necessary, the change shall contain the new identifiers. Otherwise, the changes should not imply a change in the identifier of the certificate policy.

9.13. Dispute Resolution Provisions

Claims should be addressed, by registered mail, to the GTS Management Group. Any dispute arising from the interpretation or application of the present document is governed by the Portuguese law. To resolve disputes, the parties choose the jurisdiction of the Judicial District of Funchal, excluding any other. All claims between users and the GTS TSA may be communicated to the Supervisory Authority with the purpose of the resolution of conflicts that may eventually arise.

9.14. Governing Law

The following legislation applies to Certification Authorities providers of trust services:

- EU Regulation No. 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/CE;
- Other national and European legislation on qualified trust services provision.

9.15. Compliance with Applicable Law

This document (CP) is subject to European and national laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on export or import of software, hardware or technical information.

If a court or government agency with jurisdiction on the activities covered by this CP determines that compliance with any mandatory requirement is illegal or not appropriate in the country where the CA operates, such requirement shall be considered reformulated to the minimum extent necessary to make the requirement valid and legal. This only applies to operations or issuance of certificates that are

subject to the laws of that jurisdiction. GTS commits to notify the CA/Browser Forum about the facts, circumstances, and laws involved so that the CA/Browser Forum may reassess these Guidelines accordingly.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

Relying Parties accept, in its entirety, the content of the latest version of this CP. If one or more provisions of the present document, is or tend to be invalid, void, or not enforceable in legal terms, they should be considered as non-effective. These determinations are valid, only in cases in which such provisions are not considered essential. The Management Group is responsible for assessing their essentiality. Practices adopted by the GTS TSA guarantee the independence of members of trust groups and that of the upper management, and the freedom before trade, financial and other pressures that may affect the trust of services provided. The GTS TSA ensures conditions so that their hierarchy services may be used by people with disabilities, in accordance with European Regulation 910/2016.

9.16.2. Assignment

Parties operating under this CP or applicable agreements may not assign their rights or obligations without the prior written consent of the GTS Trust Group.

9.16.3. Severability

If a provision of this CP, including limitation of liability clauses, is found to be ineffective or unenforceable, the remainder of this CP shall be construed in the sense of the original intention of the parties. Any provision of this CP that provides for a limitation of liability shall be segregable and independent of any other provision and shall be enforced as such.

9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)

GTS may claim damages and attorney's fees from a party for damages, losses and/or expenses related to the conduct of that party. The failure of GTS to enforce a provision of this CP does not waive the right of GTS to enforce the same provision thereafter or the right to enforce any other provisions of this CP. To be effective, any waiver must be in writing and signed by GTS.

9.16.5. Force Majeure

Force majeure clauses are included in the General Conditions – FO31.

9.17. Other Provisions

No stipulation.

Assinado com Assinatura
Digital Qualificada por:
TOLENTINO DE DEUS
FARIA PEREIRA
Data: 04-07-2023 15:54:45