GTS CA CERTIFICATION PRACTICE STATEMENT

Global Trusted Sign

Document Reference: DP02_GTS

Document Classification: Public

Date: 7 July 2026

Document OID:

- Practice Statement - 1.3.6.1.4.1.50302.1.1.1.2.1.0
- Principles Statement - 1.3.6.1.4.1.50302.1.1.3.2.1.0

Revisions

Version Number	Creation	Approval	Reason
	Security Administration	**Management Group**	Annual review of the document, including the correction of DN references to CN, updating of identity validation processes, strengthening of subscribers' rights, and updating of the platform's registration and security requirements.
19	Assinado com Assinatura Digital Qualificada por: CLÁUDIA BAETA DA SILVA Data: 07-07-2026 18:29:14	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Com poderes de representação de acordo com a delegação de poderes com data de 20 de Agosto de 2020. Data: 07-07-2026 18:31:07	

Table of Contents

1. Introduction

a) Scope

This document is the Certification Practice Statement and its purpose is to inform the procedures followed by Global Trusted Sign, hereinafter referred to as CA, as a qualified service provider under Regulation (EU) 2024/1183, amending Regulation (EU) No 910/2014 (eIDAS), as well as other applicable legislation and technical standard, in support of its activity of issuing qualified and advanced certificates of the GTS Certification Authority.

b) Target Audience

This document is publicly available and is intended to reach all participants related to the GTS CA.

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 Certification Practice Statement, 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 statement. The first seven chapters describe the most important procedures and practices within the digital certification of the PKI. Chapter eight describes the compliance audits. Chapter nine describes legal matters.

1.1. Overview

The practices of creation, signing, and issuance of certificates, as well as the revocation of invalid certificates, conducted by a Certification Authority (CA) are fundamental to guarantee the reliability and trust of a Public Key Infrastructure (“PKI”). This Certification Practice Statement specifies the security requirements, policies, and practices applicable by the qualified trust service provider issuing certificates. The security policies and requirements are defined in the requirements for managing the lifecycle of qualified certificates in accordance with the existing certificate policies.

1.2. Document Name and Identification

1.2.1. Revisions

This document is the Certification Practice Statement of the GTS CA, the information on which is as follows:

Document information	
Document Name	GTS CA Certification Practice Statement
Document Version	19.0
Document Status	Approved
OID	Practice Statement - 1.3.6.1.4.1.50302.1.1.1.2.1.0 Disclosure of Principles - 1.3.6.1.4.1.50302.1.1.3.2.1.0
Date of Issue	7 July 2026
Validity	7 July 2027
Location	https://pki.globaltrustedsign.com/index.html

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

1.2.2. Relevant Dates

Version ID	Version date	Reason for amendment
Version 1	31-07-2017	GTS CA Certification Practices Statement
Version 2	12-09-2017	Content Update
Version 3	29-12-2017	QtimeStamp - ETSI EN 319 421
Version 4	05-03-2018	Update of formatting and general content
Version 5	08-03-2018	Update of point 12.3
Version 6	09-01-2019	Update of information on remote validation
Version 7	02-05-2020	Update of the GTS CA hierarchy with SUBCA of advanced certificates
Version 8	24-06-2020	Update of the hierarchy of the GTS CA with SUBCA 03
Version 9	17-09-2020	Update of GTS Trust Group employee records. Update of GTS Trust Group and registrations.
Version 10	06-05-2021	Update of document structure according to RFC 3647
Version 11	23-06-2021	General update of contents
Version 12	21-07-2021	OID correction
Version 13	20-07-2022	Annual validation of the document
Version 14	15-02-2023	Update of the PKI hierarchy and review of the document
Version 15	04-07-2023	Annual verification of the document and update of values associated with telephone contacts
Version 16	06-07-2023	Update of point 4.9.7 addresses.
Version 17	05-09-2024	Annual review of the document and merger with DP04
Version 18	09-09-2025	Annual review of the document
Version 19	07-07-2026	Annual review of the document, including the correction of DN references to CN, updating of identity validation processes, strengthening of subscribers' rights, and updating of the platform's registration and security requirements.

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

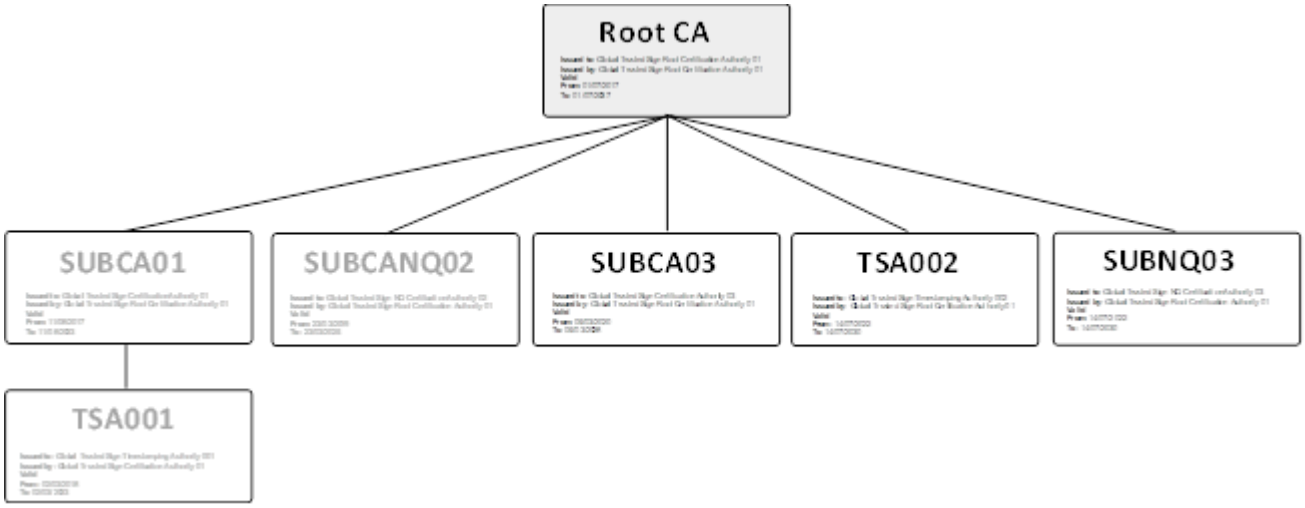
VAT Number: 511 135 610

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

ACIN-iCloud Solutions, through its Global Trusted Sign (GTS) brand, 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

[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.

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

a) GTS Root Certification Authority (GTS ROOT CA)

The GTS ROOT CA is a certification authority accredited by the National Security Office (*Gabinete Nacional de Segurança* - GNS), in accordance with Regulation (EU) 2024/1183, which amends Regulation (EU) No 910/2014 (eIDAS), as well as other applicable legislation and technical standards, and being legally authorised to issue certificates to Subordinate Certification Authorities.

GTS ROOT CA certificate:

Certificate information	
Distinguished Name	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Signature Algorithm	Sha256RSA
Serie Number	7d 9f 44 7c b2 77 97 a8 59 57 bf 11 dd 8f 99 f5
Validity	01/07/2017 a 01/07/2037
Thumbprint	70 d1 2e f7 f5 90 18 87 47 88 42 c6 4e 05 ef 2c 0a 63 92 9d
Issuer	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

b) GTS Certification Authority (GTS CA)

The Global Trusted Sign Certification Authority issues:

✓ **Qualified certificates for Website authentication (SSL/TLS)**

Website authentication services provide means that guarantee website visitors that there is a genuine and legitimate entity responsible for the website. These services contribute trust security and building when conducting online business, as users trust websites that have been authenticated, through an authenticity, ownership and confidentiality guarantee of the information transmitted. The GTS CA practice in issuing qualified certificates for website authentication meets CA/Browser Forum requirements available at http://www.cabforum.org:

- *Organisation Validation: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*;

- *Extended Validation: Guidelines for the issuance and management of Extended Validation Certificates*.

The validation of the domain of the requested certificates (domain owner, domain wildcard, and CAA Records) as defined in the CA/B Forum:

- *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.8.4.* chapter 3.2.2.

In case of inconsistency between this Practice Statement and Certification Policy and these CA/B Forum Requirements, the latter will prevail.

✓ **Certificates for qualified electronic signature**

Certificates for qualified electronic signatures enable the creation of qualified digital signatures in electronic documents with a legal effect equivalent to a handwritten signature, acting as a proof of issuance of an electronic document by a certain natural person and confirms, at least, his/her name or pseudonym, as well as the document integrity.

✓ **Certificates for electronic seals**

Certificates for electronic seals allow the creation of qualified digital signatures in electronic documents with the same legal effect of a handwritten signature, as it works as an electronic document proof of issuance by a certain legal person, certifying the document origin and integrity.

GTS CA certificates – SUBCA01:

Certificate Information	
Distinguished Name	CN = Global Trusted Sign Certification Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Signature Algorithm	Sha256RSA
Serie Number	5d f5 55 01 8c 89 45 56 59 8d cf d9 13 3b 87 ab
Validity	11/08/2017 a 11/08/2023
Thumbprint	2b 30 32 d4 9d 12 74 af 30 ab a3 ec 29 a6 a0 25 ae f6 dc bc
Issuer	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

GTS CA certificates – SUBCA03:

Certificate Information	
Distinguished Name	CN = Global Trusted Sign Certification Authority 03, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Signature Algorithm	Sha256RSA
Serie Number	1e 0a 5a 4e b2 45 99 3c 5e b9 2f 31 48 db 0c f6
Validity	11/05/2020 a 11/05/2028
Thumbprint	60 2f 17 18 96 72 78 f5 88 4f 33 16 f2 65 9b c1 f3 cc b2 46
Issuer	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

c) 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 (timestamping 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 synchronised, 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

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

The GTS NQ CA issues advanced non-qualified electronic signature certificates, in its capacity as a Trust Service Provider, in accordance with the applicable requirements of Regulation (EU) No 910/2014 (eIDAS), in its consolidated version, as amended by Regulation (EU) 2024/1183, as well as with the standards ETSI EN 319 401 – Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers and ETSI EN 319 411-1 – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 1: General Requirements, in their current versions.

GTS NQ CA - SUBCANQ02 certificate:

Certificate Information	
Distinguished Name	CN = Global Trusted Sign NQ Certification Authority 02, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Signature Algorithm	Sha256RSA
Serie Number	7e 88 a8 ed 54 02 9f c6 5c 96 00 8e 0a cf bd c1
Validity	23/03/2019 a 23/03/2025
Thumbprint	7e 55 0f f3 8f 70 2e eb 5d 8f f0 e2 02 75 78 3f be 83 57 38
Issuer	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

GTS NQ CA - SUBCANQ03 certificate:

Certificate Information	
Distinguished Name	CN = Global Trusted Sign NQ Certification Authority 03, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT
Signature Algorithm	sha256RSA
Serie Number	5b 12 f7 4a cb ca 73 e0 62 cf f2 13 84 35 c5 64
Validity	14/07/2022 a 14/07/2030
Thumbprint	13 c5 be fc 66 be 0f fe 82 97 97 ec 44 5f a9 e4 96 d2 f1 a8
Issuer	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

1.3.2. Registration Authority

The Registration Authority (RA) is the entity responsible for approving the distinguished names (CN) 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 in document FO23_GTS - Terms and Conditions for GTS Certificates

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 Registration Authorities, since there is no contract with third parties to carry out domain validation of SSL certificates and of the identity of advanced and qualified certificates.

1.3.3. Subscribers

Within the scope of this certification practice statement, subscribers/holders are all final users to whom certificates have been attributed by the Global Trusted Sign PKI. The holders of certificates issued by Global Trusted Sign 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 (organisations);
- 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.

Access to the Global Trusted Sign services requires the user to complete prior registration on the Global Trusted Sign platform.
Subscribers undertake to keep their contact details up to date, in particular their email address.

- Loss of access to the registered email address may prevent the renewal or management of certificates and may result in their revocation for security reasons.

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 Global Trusted Sign 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 by Regulation (EU) 2024/1183, amending Regulation (EU) No 910/2014 (eIDAS) of the European Parliament and of the Council.

b) External Entities

Activities of service providers that support Global Trusted Sign 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 Global Trusted Sign.

c) Conformity Assessment Body

The Conformity Assessment Body (CAB) is the entity defined in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008, as amended, laying down the requirements for the accreditation of conformity assessment bodies, accredited in accordance with that Regulation to carry out the conformity assessment of Qualified Trust Service Providers (QTSPs) and the qualified trust services they provide, in accordance with Regulation (EU) 2024/1183, amending Regulation (EU) No 910/2014 (eIDAS), as well as the other applicable legislation and technical standards.

1.4. Certificate Usage

Certificates issued by the Global Trusted Sign PKI, and in the GTS ROOT CA trust hierarchy, 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 based on the use of public key cryptography, supported by the Public Key Infrastructure (PKI) provided by Global Trusted Sign, which establishes the chain of trust required for the issuance and validation of digital certificates. Relying Parties may verify the certification path of a certificate issued by the GTS CA, thereby confirming its authenticity, integrity, and the identity of its holder. Qualified certificates issued by the GTS CA are issued in accordance with this Certification Practice Statement and Certificate Policy and comply with the requirements established by Regulation (EU) 2024/1183, amending Regulation (EU) No 910/2014 (eIDAS), as well as all other applicable legislation and technical standards.

The qualified certificates for website authentication issued by the GTS CA are used by the various holders, systems, applications, mechanisms and protocols, with the aim of establishing web data communication via SSL/TLS protocols.

This guarantees efficient and secure electronic communications, while at the same time addressing concerns of users about the reliability of certificates.

1.4.1. Appropriate Certificate Uses

The requirements and rules defined in this document apply to all certificates issued by the Global Trusted Sign PKI.

a) Qualified Certificates for Website Authentication

Qualified certificates for website authentication issued by the GTS CA are used by different holders, systems, applications, mechanisms and protocols, in order to establish Web based data communication through SSL/TLS protocols. Qualified Certificates for Website Authentication are intended to:

- Identify the legal entity that controls a website: it provides reasonable assurance to the user of an Internet browser that the site to which the user will access is controlled by a legal entity identified in the certificate by its name, registered office, registration in the *Instituto de Registos e Notariado* (Institute of Registries and Notaries), or any other derived information;
- Allow encrypted communications with a website: it facilitates the exchange of encryption keys to allow transmission of encrypted information through Internet, between an Internet browser user and a website.
- Prevent phishing attacks and other frauds of the identity used in the certificates;
- Support companies that have been targeted in phishing or identity fraud by making available to users a tool for its identification;

- Support to the security forces in their investigations of phishing and other attacks of identity fraud, contributing, as appropriate, the contact, research, and legal actions against the Holder.

Relying Parties can verify the chain of trust of a certificate issued by the GTS CA, thus guaranteeing the authenticity and identity of the holder.

b) Qualified Certificates for Signature and Electronic Seals

Qualified certificates for electronic signature and electronic seals issued by Global Trusted Sign are used by different holders, systems, applications, mechanisms and protocols, in order to allow the probatory signature on documents by natural and legal persons. Qualified electronic signature certificates should be used for the creation of digital signatures in electronic documents with legal effect equivalent to a handwritten signature. This use serves as a prove of emission of an electronic document by a specific natural person and confirms, at least, his/her name or pseudonym, as well as the integrity of the document. In the case of certificates for electronic seals, the use is similar to qualified signature, however, issuance tests are applied to confirm their issuance by a legal person, certifying the origin and the integrity of the document. The subscriber is responsible for the content of all transactions made through the service.

c) Advanced Certificates for signature and electronic seals

Advanced digital certificates offer a high level of confidence; nevertheless, they do not guarantee the probative value of qualified certificates.

These certificates can be used to:

- Perform online authentication securely;
- Sign emails;
- Sign documents without legal probative value.

1.4.2. Prohibited Certificate Uses

Certificates issued in the GTS CA hierarchy of trust shall not be used for any purpose outside the scope of the uses described above, with the exception of being able to be used in other contexts when legally foreseen in the applicable legislation. The certification services provided by the GTS CA do not guarantee compliance with high availability and resilience requirements, which qualify them for use in critical services or infrastructures, such as those related to the operation of medical, nuclear, air traffic control, rail traffic control facilities, or any other activity where a failure could lead to death, personal injury or serious damage to the environment.

Qualified certificates for website authentication issued by the GTS CA focus on the identity of the Certificate Holder, and not on his/her behaviour. Therefore, a web authentication certificate does not give any guarantees as to whether:

- The Holder identified in the certificate is actually providing service;
- The Holder identified in the certificate complies with applicable legislation;
- The Holder identified in the certificate is reliable, honest or ethical in carrying out its business;
- That it is 'safe' to establish a business relationship with the Holder identified in the certificate

1.5. Policy Administration

1.5.1. Organization Administering the Document

The management of the GTS CA Certification Practice Statement is responsibility of the Global Trusted Sign Security Administration Group.

1.5.2. Contact Entity

	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] (GTS - Option 3) [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 Certification Practice Statement (CPS) 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 CA Management Group, for its approval.

1.5.4. CPS Approval Procedures

The validation of this CPS and/or related CP and all corrections or updates are performed by the Global Trusted Sign Security Administration. All corrections or updates are published as new versions of this CPS and/or related CP, replacing any CPS and/or related CP previously defined. The Global Trusted Sign Security Administration is responsible for determining when the changes on the CPS and/or respective CP will result in a change on the object identifiers (OID) of the CPS and/or respective CP. After validation, the CPS (and/or its CP) is submitted to the Global Trusted Sign 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 a) 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, issued by a qualified trust service provider, which meets the requirements laid down in Annex I to Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183.
Qualified Certificate for Website Authentication	Certificate for website authentication, which is issued by a qualified trust service provider that meets the requirements laid down in Annex IV to Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183.
Qualified Certificate for Electronic Seals	Certificate for electronic seals, which is issued by a qualified trust service provider that meets the requirements laid down in Annex III to Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183.
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.

Definitions	
Term	**Definition**
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.
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, as amended by Regulation (EU) 2024/1183.
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, as amended by Regulation (EU) 2024/1183.
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, as amended by Regulation (EU) 2024/1183.
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 (CN) 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.

Definitions	
Term	**Definition**
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.
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 as being accredited in accordance with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, 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.

Definitions	
Term	**Definition**
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.
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, as amended by Regulation (EU) 2024/1183.
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
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

- ✓ 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, as amended, including the amendments introduced by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024
- ✓ ETSI EN 319 411-1 v1.5.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
- ✓ ETSI EN 319 411-2 v2.6.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

- ✓ ETSI 319 412 v1.4.2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
- ✓ ETSI EN 319 401 v3.1.1: General policy requirements for Trust Service Providers;
- ✓ RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate and CRL Profile, 2008
- ✓ 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

Not stipulated.

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
- 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 CA conducts the following publications, with the following frequency of publication:

- GTS CA 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 GTS CA ensures the issuance of certificates with a Distinguished Name (CN) X.509 to all holders who submit documentation containing a verifiable name according to what is set in RFC 5280. The allocation of names follows the conventions below:

- Certificates for website authentication assign a qualified name of the domain and/or trust service, according to ETSI EN 319 412-4 v1.2.1;
- Certificates for qualified signature of natural persons assign the real name of the holder, according to ETSI EN 319 412-2 v2.3.1.
- Certificates for qualified signature of natural persons in association with legal persons assign the name of the holder and the relationship with the legal person, according to ETSI EN 319 412-2 v2.3.1;
- Certificates for electronic seals assign the name of the legal person, according to ETSI EN 319 412-3 v1.3.1.

Name allocation complies with the requirements specified in the certificate policies, with identification in each of the policies:

Policy Identifier	OID
Root CA Certificate Policy	1.3.6.1.4.1.50302.1.1.2.1.1.0
SSL EV Certificate Policy	1.3.6.1.4.1.50302.1.1.2.2.1.0
SSL OV Certificate Policy	1.3.6.1.4.1.50302.1.1.1.2.1.1
Qualified Signature Certificate Policy	1.3.6.1.4.1.50302.1.1.1.2.1.2
Electronic Seals Certificate Policy	1.3.6.1.4.1.50302.1.1.1.2.1.3
Advanced Signature Certificate Policy	1.3.6.1.4.1.50302.1.1.2.6.1.0
Advanced Electronic Seals Certificate Policy	1.3.6.1.4.1.50302.1.1.2.7.1.0
Timestamp Policy	1.3.6.1.4.1.50302.1.1.2.3.1.0

3.1.1. Types of Names

The GTS CA guarantees that the allocation of names complies with the requisites specified in the certificate policies for each type of profile presented. The various types of certificates may contain the following fields in the CN:

Attribute	Code	Rules
Country	C	Code of the certificate holder's country.
Organization	O	This field corresponds to the organization (or equivalent) to which the certificate holder belongs.
Organization Unit	OU	This field corresponds to the information regarding the organization unit (or equivalent) to which the certificate holder belongs.
Common Name	CN	Unique name of the certificate holder. In the case of web servers, it will be designated by FQDN (CN = "FQDN".), being forbidden its designation by the IP address or local domains. In the case of qualified signature certificates, they contain the name of the holder or the pseudonym. In the case of electronic seals certificates, they contain the name of the legal person.
Serial Number	serialNumber	Follows ETSI EN 319 412 recommendations.

3.1.2. Need for Names to be Meaningful

The GTS CA ensures that the names used in the certificates it issues identify in a significant and clear manner their holders, ensuring that the CN used is appropriate for a certain holder and that the ***Common Name*** component of the CN represents it in a manner that can be easily identified by the interested parties. The GTS CA ensures that any ***Common Name*** field in the Subject CN 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 CA 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 CA 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 CA, there are controls that ensure that the CN 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

CNs issued by the GTS CA 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 CN.

3.2. Initial Identity Validation

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

Verification of the applicant's identity may be carried out using one or more of the methods set out in Article 24(1) of Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183, including remote identification by videoconference pursuant to point (d), or other recognised remote identification methods, provided that they ensure a level of reliability equivalent to physical presence and comply with applicable legal and regulatory requirements and technical standards.

The applicant's identity may also be verified using a valid qualified certificate issued by a Qualified Trust Service Provider, or by any other electronic identification means provided for in Article 24(1) of Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183, provided that it complies with the applicable requirements for the issuance of qualified certificates.

3.2.1. Method to Prove Possession of Private Key

In cases in which the GTS CA 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

CNs issued by the GTS CA 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. The GTS CA validates the authenticity of the data through one of the following ways:

a) By using documents issued by government agencies (Commercial Registry, Electronic Commercial Registry, etc.);

b) Authentication of the certificate request form containing the data of the organisation, by a legal entity with powers for such an act (lawyer, notary or solicitor);

c) A periodically updated third party database;

d) Method of Proof of Email Address Control

When an email address is included in the ***Common Name*** or ***Subject Alternative* Name** attributes of a digital certificate, the subscriber shall prove that he/she controls the email address. For this, the GTS CA performs a challenge-response procedure, which consists in generating a token and sending it by email to the email address to be included in the certificate. To prove the control of the email address, the subscriber must click on the link containing the token, which is included in the email. The CA receives the reply and the proof of email address control is successfully completed. This procedure is also carried out to confirm the email address of the subscriber included in the certificate request form (subscriber's email contact);

e) Domain Name / Address Validation Method

The GTS CA validates the right of use or control by the domain name applicant, which shall be listed in the ***Common Name*** and ***Subject Alternative Name*** of the certificate, using at least one of the procedures described in section 3.2.2.4 of the CA/B Forum Baseline Requirements.

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 Global Trusted Sign 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.

In the issuance of SSL OV (Organisation Validation) / EV (Extended Validation) component certificates, the legal existence of the requesting entity is verified through consultation of reliable information sources. For this purpose, public registers (https://eportugal.gov.pt), commercial databases such as InformaDB (https://www.informadb.pt/), or other deemed appropriate official sources, such as the tax authority databases (https://www.portaldasfinancas.gov.pt/), may be used in order to confirm the legal existence, identity, legal status and, where applicable, the authority of the entity to apply for the certificate.

For EV certificates the operational activity of the entity is verified in a reliable manner, as well as to which category of entity it belongs according to the classification established in the policies defined by the CA/Browser Forum in the "*Guidelines for the Issuance and Management of Extended Validation Certificates*" (*Private Organisation, Government Entity, Business Entity and Non-Commercial 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 organisation 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.

Global Trusted Sign does not accept fictitious entity names that cannot be confirmed in the aforementioned databases used as a means of verifying identity.

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

- The verification of the identity of the subscribers and/or holders will be carried out by the working group of Administrators, after confirmation of payment and document validation, and can be done in the following ways:
- **In person**, in Portuguese or English, by prior appointment, at the company's registered office in the Autonomous Region of Madeira or at its premises in Lisbon, Porto or Ponta Delgada. The applicant must present a valid original identification document, and identity verification shall be performed by two Registration Administrators, in accordance with GTS internal procedures. This identification method is carried out in accordance with point (a) of Article 24(1) of Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183; or
- **Remotely**, through remote identification, including videoconference or other remote identification methods implemented by GTS and permitted under applicable legislation, in

Portuguese or English, by prior appointment. The applicant, or duly authorised legal representative of the legal person, must be physically present during the identification process and must present a valid original identification document for verification of their identity prior to the issuance of the qualified certificate. Remote identification is carried out through a technological platform that complies with the applicable legal, regulatory and technical requirements, ensuring a level of reliability equivalent to physical presence, in accordance with point (d) of Article 24(1) and the "substantial" or "high" assurance levels set out in Article 8 of Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183, as well as with the requirements defined in Order No 154/2017 of the National Security Authority and other applicable legislation and technical standards; or

- **Through a notified electronic identification means**, in particular using the Portuguese Citizen Card authentication certificate or the Digital Mobile Key (Chave Móvel Digital – CMD), via the Autenticacao.gov.pt portal, provided that the applicant holds a compatible electronic identification document and digital certificate. This method is available to Portuguese citizens and is used in accordance with point (c) of Article 24(1) of Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183; or
- **Through the use of a valid qualified electronic signature certificate or a qualified electronic seal certificate**, issued by a Qualified Trust Service Provider, for the purpose of verifying the applicant's identity, in accordance with point (d) of Article 24(1) of Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183. This method is applicable, in particular, to qualified certificate renewal processes, provided that the applicable legal and regulatory requirements continue to be met.

a) Natural Person Identification

If the holder is a natural person, the identity may be verified through:

- Names and surnames (in accordance with national practices for the identification of persons);
- Date and place of birth;
- Nationally recognized identification document that allows to distinguish the holder from others with the same name;
- Documents with probative value equivalent to physical presence.

If the holder is a natural person in associated with a legal person:

- Names and surnames (in accordance with national practices for the identification of persons);
- Date and place of birth;
- Nationally recognized identification document that allows to distinguish the holder from others with the same name;
- Documents with probative value equivalent to physical presence;

- Full name and data of the legal person;
- Evidence of the association of the physical person with the legal person that will appear in the attributes of the certificate.

If the holder is a natural person of the Professional Type:

- Names and surnames (in accordance with national practices for the identification of persons);
- Date and place of birth;
- Nationally recognized identification document that allows to distinguish the holder from others with the same name;
- Documents with probative value equivalent to physical presence;
- Indication with evidence of the Profession exercised;
- License number of the professional association and submission of proofs;
- Organization / Entity where the profession is practiced, with evidence to be submitted.

b) Legal Person Identification

If the holder is the representative of a legal person, the identity may be verified through:

- Names and surnames of the applicant (in accordance with national practices for the identification of persons);
- Date and place of birth;
- Nationally recognized identification document that allows to distinguish the holder from others with the same name;
- Documents with probative value equivalent to physical presence;
- Data of the legal person:
  - Full name of the legal person;
  - Address;
  - Tax identification number (TIN);
  - Access code of the Electronic Commercial Registry (where applicable) or minutes of taking office, accompanied by the statutes.
- In case the applicant is not the legal representative of the legal person, a power of attorney for issuing the electronic seal is requested.

If the holder is a natural person of the professional type in association with a legal person:

- Names and surnames (in accordance with national practices for the identification of persons);
- Date and place of birth;
- Nationally recognized identification document that allows to distinguish the holder from others with the same name;
- Documents with probative value equivalent to physical presence;
- Full name and data of the legal person;

- Evidence of the association of the natural person with the legal person that shall appear in the attributes of the certificate;
- License number of the professional association and submission of proofs;
- Exercised Responsibilities/Position;
- Area/Department to which belongs.

c) Device or System Identification

Registration and authentication process will be guaranteed by the Registry Administration Working Group to properly register final users of the certificate, through all necessary means for an adequate and legal identification of the applicant. Among the actions to be taken to meet this goal, are the following:

- Verification of documents officially recognized by the State in which the Subscriber (natural or legal person) is registered:
- Full name;
- Contact information, including contact address;
- Unique and legal identification.

Identification must be authenticated through tests of identity in accordance with the following provisions:

- To be officially recognized in the jurisdiction in which the subscriber is registered;
- To indicate the complete Subscriber name and address official;
- To have at least a proof of identity that contains a photograph of the subscriber;
- To indicate a unique registry number within the jurisdiction that had been issued.

Global Trusted Sign shall verify whether each applicant has the right or entitlement to obtain the requested certificate. In order for qualified certificates for website authentication with extended validation to be issued within the Global Trusted Sign shall trust hierarchy, the GTS CA shall verify the identity and address of the requesting legal person, and confirm that the stated address corresponds to that set out in the articles of association or to the place where its activities are carried out.

3.2.4. Non-Verified Subscriber Information

All information in the certificate 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 Global Trusted Sign 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 (PKI) allow for the automatic renewal of certificates prior to the expiry of their respective validity period, while maintaining the trust relationship previously established with the subscriber.

In Global Trusted Sign, there is no concept of certificate renewal. Whenever it is necessary to replace a certificate, including in cases where its validity period is approaching expiry, a **new issuance (re-issuance)**, is performed, subject to the applicable issuance process and compliance with the legal, regulatory and procedural requirements in force. Each re-issuance constitutes a new certificate issuance, resulting in a new certificate with a new validity period and, where applicable, a new verification of the applicant's identification data, in accordance with this Certification Practice Statement and Certification Policy.
Consequently, any request for certificate replacement is treated by Global Trusted Sign as a new certificate issuance request, with no automatic certificate renewal process in place.

3.3.2. Identification and Authentication for Re-Key after Revocation

Although the request may be motivated by the approaching expiry of an existing certificate, **Global Trusted Sign does not operate a certificate renewal process**. In such cases, the request is always treated as a **new issuance (re-issuance)**, as each certificate constitutes a new electronic credential issued with a new validity period and a new serial number, and is subject to the issuance process defined in this Certification Practice Statement and Certification Policy, as well as to compliance with the applicable legal, regulatory and procedural requirements.
Where applicable, Global Trusted Sign may require the subscriber to use the same authentication means used in the initial application process or to undergo a new identity verification, in accordance with the requirements laid down in Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183, and with the applicable ETSI standards.

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 CA for the issuance of certificates begins with the acquisition of the requested certificate and the subsequent submission of the corresponding application, by completing the form for the type of certificate requested and accepting the terms and conditions established by the GTS CA.

The form must be signed by the applicant, and submission may be carried out:

- in paper form, with a handwritten signature, in which case the original signed documents must be sent to Global Trusted Sign by postal mail; or
- electronically, using a qualified electronic signature, in which case the submission of paper documents is waived, provided that the applicable legal, regulatory and procedural requirements are met.

The issuance of the certificate is subject to the verification of the applicant's identity, the validation of the information provided, and compliance with the requirements set out in this Certification Practice Statement and Certification Policy, as well as in the applicable legislation and technical standards.

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 Global Trusted Sign representative.

4.1.2. Enrollment Process and Responsibilities

After receiving the documentation, a process of validation of the information and identity of the holder and, when applicable, requesting entity is initiated. This process is always carried out by 2 Registry Administrators, with the purpose of verifying the authenticity of the data provided, depending on the type of certificate requested. Global Trusted Sign does not use external registration entities to provide the registration service. In the case of Web/SSL certificates, the form shall be accompanied during its

submission, by a CSR (Certificate Signing Request) that shall contain information for the certificate fields, which shall coincide with the fields entered in the form.

Note: A certificate request does not imply its obtainment in case the applicant does not meet the requirements established in this CPS. 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 Global Trusted Sign 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. For Website Authentication certificate requests, GTS also checks the relevant CAA records when submitting the certificate request and immediately before issuing the certificate. The CA acts in accordance with the CAA records, if any. The GTS CA identification domain in the CAA records is globaltrustedsign.com. The GTS CA limits the reuse of supporting information for certificate renewal, in accordance with section 11.14.3 "*Age of Validated Data*" of the CA/ Browser Forum *Guidelines for the Issuance and Management of Extended Validation Certificates*.

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

Global Trusted Sign has 60 minutes after validating the identity and suitability of the subscriber and the proper collection to proceed with the issuance and delivery of the web authentication certificate. For the remaining requests, the deadline for issuing a certificate is defined in the respective terms and conditions: FO31 – General terms and conditions and FO23 – Certificates terms and conditions.

4.3. Certificate Issuance

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

4.3.1. CA Actions during Certificate Issuance

The certificate issuance process is always carried out by two Registry Administrators, in order to guarantee double authentication. Only in this way, the authenticity of the data provided is validated and confirmed.

The e-seal and signature qualified certificates are issued through the interaction of the Certification Authority with a cryptographic module in hardware (Hardware Secure Module - HSM), based on the type of applicable certificate policy. The public key certificate is stored in the HSM. In the case of certificates for website authentication (OV or EV), the issued certificate begins its validity at the moment it is issued and the subscriber of the certificate is notified via electronic mail, and the public key certificate is sent through this channel. The delivery of the certificate requires an acceptance which is carried out in accordance with section 4.4. Denominations not recognized by the ICANN (Internet Corporation for Assigned Names and Numbers) will not be accepted, for certificates for websites authentication.

In the case of certificates for qualified signature or electronic seal, the issuance of the certificate is carried out by its holder after the verification of the identity of the holder at the time of its issuance through:

- Access credentials to the GTS Portal
- Reception of the OTP code in the email configured in the registry of the holder

Holders have 180 days to issue any type of certificate, otherwise they must repeat the videoconference.

Advanced Certificates are issued by the Registry Administrators and are available for download in the personal area of the Global Trusted Sign portal, once the authentication is done. To use the certificate, a PIN will be sent via the Global Trusted Sign portal or by SMS to the mobile number provided by the certificate holder for this purpose at the time of purchase of the product. This certificate can be downloaded as many times as necessary.

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 CA does not publish the list of issued certificates.

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

The GTS CA 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 CA.

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 CA supplies in this CPS information about the appropriate services available to verify the validity status of the certificate, such as OCSP and CRL.

4.6. Certificate Renewal

The GTS CA does not have a certificate renewal process. Whenever it is necessary to replace a certificate, including in cases where its validity period is approaching expiry, the subscriber shall submit a new issuance request (re-issuance), while retaining, where applicable, the same parameters as the previous certificate.

Each re-issuance involves the generation of a new cryptographic key pair and the issuance of a new certificate, with a new serial number and a new validity period.

The re-issuance process follows the same authentication, identification and validation procedures applicable to the initial issuance. Previously accepted identification means may be reused where permitted by applicable law and by this Certification Practice Statement and Certification Policy.

4.6.1. Circumstance for Certificate Renewal

Not stipulated.

4.6.2. Who may Request Renewal

Not stipulated.

4.6.3. Processing Certificate Renewal Request

Not stipulated.

4.6.4. Notification of New Certificate Issuance to Subscriber

Not stipulated.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Not stipulated.

4.6.6. Publication of the Renewal Certificate by the CA

Not stipulated.

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

Not stipulated.

4.7. Certificate Re-Key

4.7.1. Circumstance for Certificate Re-Key

The Certificate Re-Key process is not supported by the GTS CA.

4.7.2. Who may Request Certification of a New Public Key

Not stipulated.

4.7.3. Processing Certificate Re-Key Requests

Not stipulated.

4.7.4. Notification of New Certificate Issuance to Subscriber

Not stipulated.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Not stipulated.

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

Not stipulated.

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

Not stipulated.

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 CA.

4.8.1. Circumstances for Certificate Modification

Not stipulated.

4.8.2. Who May Request a Certificate Modification

Not stipulated.

4.8.3. Processing Certificate Modification Requests

Not stipulated.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not stipulated.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not stipulated.

4.8.6. Publication of the Modified Certificate by the CA

Not stipulated.

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

Not stipulated.

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 CA.

Access to the services provided by Global Trusted Sign requires the user to register on the Global Trusted Sign platform by creating a user account with personal and non-transferable credentials.

The subscriber is responsible for keeping their email address active and up to date, as this is the main channel of communication for notifications regarding renewal, suspension or revocation.
The loss of or inability to access the registered email address may prevent communication with the subscriber and, for security reasons, may justify the revocation of the certificate.

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

a) A certificate shall be revoked within 24 hours for one of the following reasons:

- The Subscriber requests in writing that the CA revoke the Certificate;
- The Subscriber notifies the CA that the initial 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;
- The CA is informed of a demonstrated or proven method that can easily calculate the Private Key of the Subscriber based on the Public Key in the Certificate;
- The CA has evidence that the validation of the domain authorisation or control for any fully qualified domain name or IP address in the certificate should not be considered;
- 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 CA receives notification or has implied knowledge of any circumstance that indicates that the certificate's email address is no longer legally authorise;
- 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 no longer meets the requirements set out in Section 6.1.5 and Section 6.1.6;
- The CA has evidence that the Certificate has been misused;
- Cease of activities;
- Inaccuracies or changes to the data supplied;
- The CA is informed that the Subscriber has violated one or more of his/her material obligations under the Terms and Conditions of Use;

- The CA is informed of any circumstance indicating that the use of a fully qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right of a Domain Name Registrar to use the Domain Name, or a relevant licence or service agreement between the Domain Name Registrar and the applicant has terminated, or the Domain Name Registrar has not renewed the Domain Name);
- Breach of responsibilities under the CPS by the GTS ROOT CA / GTS CA or by the holder;
- The CA is informed that the Certificate was not issued in conformity with these Requirements or with the Certificate Policy or Certification Practices Statement of the CA;
- The CA determines or is informed that any of the information contained in the Certificate is inaccurate;
- Whenever there are credible reasons that induce that the certification services may have been compromised in such a way that they place in question the reliability of the certificates;
- The right of the CA to issue certificates under the scope of these Requisites has expired or was revoked or terminated, unless the CA has taken measures to maintain the CRL/OCSP Repository;
- The CA is aware that a Subscriber has breached one or more of his/her material obligations under the Subscriber Agreement or Terms of Use;
- Revocation is required in accordance with the Certification Policy and/or Certification Practices Statement of the CA;
- Whenever it is determined that, for some reason, certificates were not issued in accordance with the GTS Certificate Policy or Certification Practices Statement;
- The CA is informed of a demonstrated or proven method that puts the Private Key of the Subscriber at risk or if there is clear evidence that the specific method used to generate the Private Key was defective;
- By legal or administrative resolution;
- Whenever the GTS CA receives notification or has implied knowledge of any circumstance that indicates that the certificate's email address is no longer legally authorised.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate.

The Issuing CA shall revoke a Subordinated CA Certificate within seven (7) days for one or more of the following reasons:

- The Subordinate CA requests the revocation in writing;

- The Subordinate CA notifies the Issuing CA that the original certificate request was not authorised and does not grant authorisation retroactively;
- The Issuing CA has evidence that the Private Key of the Subordinate CA corresponding to the Public Key in the Certificate has suffered a Key Compromise or no longer meets the requirements set out in Section 6.1.5 and Section 6.1.6;
- The Issuing CA has evidence that the Certificate has been misused;
- The Issuing CA is informed that the Certificate was not issued in conformity with or that the Subordinate CA did not comply with this document or with the applicable Certificate Policy or Certification Practices Statement;
- The Issuing CA determines that any information in the certificate is inaccurate or misleading.
- 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 CA will process the revocation request in the next 24 (working) 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, 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. The CRL is updated every 6 hours, which is issued every 24 hours or whenever there is a revocation of the certificates issued, in which case a new CRL is issued immediately. The availability in the repositories is done in a period no longer than 30 minutes, 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/subca/gts_subca_crl.crl
- https://pk2.globaltrustedsign.com/download/crl/subca/gts_subca_crl.crl
- https://pki.globaltrustedsign.com/download/crl/subca/gts_subca_03_crl.crl
- https://pki02.globaltrustedsign.com/download/crl/subca/gts_subca_03_crl.crl
- https://pki.globaltrustedsign.com/download/crl/subca_nq/gts_subcanq02_crl.crl
- https://pki02.globaltrustedsign.com/download/crl/subca_nq/gts_subcanq02_crl.crl
- https://pki.globaltrustedsign.com/download/crl/subca_nq/gts_subnq03.crl
- https://pki02.globaltrustedsign.com/download/crl/subca_nq/gts_subnq03.crl

4.9.8. Maximum Latency for CRLs (if applicable)

Global Trusted Sign 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

The GTS CA 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

Not stipulated.

4.9.12. Special Requirements Re-Key Compromise

In addition to the reasons mentioned in section 4.9.1 of this Certification Practices Statement, 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

GTS does not support suspension of the certificates.

4.9.14. Who can Request Suspension?

Not stipulated.

4.9.15. Suspension Request Procedure

Not stipulated.

4.9.16. Limits on Suspension Period

Not stipulated.

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

Not stipulated.

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 CA 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 CA 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. Facility, Management, and Operational Controls

5.1. Physical Security Controls

5.1.1. Site Location and Construction

The GTS CA was designed to provide a safe environment capable of protecting the systems that support the activities of the ROOT CA. Global Trusted Sign 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. Global Trusted Sign 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, Global Trusted Sign 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 organisation 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 Trust 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 organisation 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 authorised individual and with functions established in the TSP's organisation, to which only the individual can have access.

5.1.3. Power and Air Conditioning

The Global Trusted Sign secure environment is equipped with redundant systems, ensuring continuous operation 24 hours a day, 7 days a week:

- 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 are equipped with appropriate mechanisms (such as flood detection systems) to minimise the impact of flooding on Global Trusted Sign systems.

5.1.5. Fire Prevention and Protection

The Global Trusted Sign secure environment is equipped with the necessary mechanisms to prevent and extinguish fires or other incidents involving flames or smoke. These mechanisms comply with applicable 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 activity of issuing digital certificates by Global Trusted Sign, as a certification authority for qualified certificates, 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 Global Trusted Sign. 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 Global Trusted Sign activities, to ensure that the infrastructure is always available and operational, and forecasting future needs that may arise from Global Trusted Sign 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 Global Trusted Sign. This group has the following responsibilities:

- Definition of documentation related to Global Trusted Sign information security practices
- Definition of procedures related to cryptographic keys management
- To ensure that all Global Trusted Sign 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 Global Trusted Sign
- 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 internal compliance analysis with applicable national and European standards governing the activities of Global Trusted Sign as a Qualified Trust Service Provider, and authorised to access and monitor system activity logs. This group is responsible, in particular, for:

- 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 at least 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 Global Trusted Sign, 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 of any Global Trusted Sign working group shall meet the following requirements:

- Proof of qualification and experience for the performance of the respective duty
- Ensure confidentiality related to Global Trusted Sign sensitive information or identification data of holders
- Guarantee that they do not perform functions that may arise a conflict with their responsibilities concerning Global Trusted Sign 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, the introduction of new tools, or the modification of existing procedures shall trigger an appropriate training process for all working groups. In addition, training sessions shall be provided to members of the Certification Authority whenever the Global Trusted Sign Certification Policies or Certification Practice Statement are amended. These requirements shall be taken into account to ensure the intended level of knowledge necessary for the effective fulfilment of the responsibilities assigned to the different working groups.

5.3.5. Job Rotation Frequency and Sequence

Not stipulated.

5.3.6. Sanctions for Unauthorized Actions

All unauthorised actions and any actions in violation of the Global Trusted Sign Certification Practice Statement and Certification Policy shall be subject to disciplinary measures, whether committed intentionally or as a result of negligence. In addition, and depending on the severity 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 the Global Trusted Sign Certification Policies, the GTS Certification Practice Statement, documentation describing responsibilities, duties and tasks depending on the function, as well as additional technical documentation concerning the software and

hardware used by the Global Trusted Sign Certification Authority, shall be made available to members of the working groups.

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, whether successful or unsuccessful, to access sensitive resources of the Global Trusted Sign Certification Authority;
- Attempts, whether successful or unsuccessful, to modify security parameters;
- Attempts, whether successful or unsuccessful, to create, modify, or delete system accounts;
- Attempts, whether successful or unsuccessful, to start and end of session;
- Attempts, whether successful or unsuccessful, of transactions related to the request, issuance, renewal, modification, suspension and revocation of certificates and keys;
- Attempts, whether successful or unsuccessful, to generate, issue or update the CRL;
- Attempts, whether successful or unsuccessful, to create, modify or delete information of certificates holders;
- Attempts, whether successful or unsuccessful, to access GTS CA High Security Zones.

The record of events, whether generated automatically or manually, shall contain at least information such as the event date and time, category, description and serial number, as well as the identification of the agent responsible for the event.

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 CA 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 no significant changes occur in the GTS CA global environment, vulnerability assessments shall nevertheless be carried out in order to minimise or eliminate potential attempts to breach system security. The results of these assessments shall be reported to the responsible persons, so that they may review them and, where appropriate, approve an implementation plan and the remediation of identified vulnerabilities.

5.5. Records Archival

Global Trusted Sign ensures the archiving of records relevant to the provision of trust services, in order to guarantee their integrity, authenticity, confidentiality and availability throughout the retention period defined in this Certification Practice Statement, as well as in applicable legislation.
The records subject to archiving include, in particular, records relating to certificate issuance, re-issuance, suspension and revocation requests, applicant identification and authentication processes, operations performed by Registration Administrators, security events, audit logs, and any other elements necessary to demonstrate compliance with the services provided.
Archived records are protected against alteration, destruction, unauthorised access and loss, and are retained for the legally and regulatorily applicable retention periods

5.5.1. Types of Records Archived

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

- Audit logs 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 CA must ensure the record of the date and time of the moment, based on a secure time source.

5.5.6. Archive Collection System (Interna 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

Not stipulated.

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 CA, the following procedures shall be applied:

- 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 the European Union Agency for Cybersecurity (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 CA or its subscribers become insufficient for their intended purpose, the GTS CA shall:

- Inform all holders and other entities with which the GTS CA 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 CA data necessary to resume operations is copied and stored in safe and adequate locations to allow the proper return to operations of GTS CA 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 CA;
- 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 CA, 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 CA activity, the GTS CA 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 CA is processed in accordance with the requisites and algorithms defined in this policy.

6.1.1. Key Pair Generation

6.1.1.1. CA 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.

6.1.1.2. RA Key Pair Generation

Not stipulated

6.1.1.3. Subscriber Key Pair Generation

See section 4.5.1.

6.1.2. Private Key Delivery to Subscriber

Not stipulated.

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 CA 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

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

6.2.1. Cryptographic Module Standards and Controls

The GTS CA 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 CA cryptographic module). The GTS CA 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, Procedural Controls, and section 14.3, Staff Safety 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 Global Trusted Sign 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 CA 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 CA 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 CA 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 GTS 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 GTS 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 CA 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 CA 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 CA has a minimum validity of 1 year, and a maximum validity of 3 years;
- An EV or OV SSL certificate has a maximum validity of 398 days.
- All certificates issued by GTS are valid from the moment they are issued until they expire. No certificate issued for a server can exceed a validity period of more than 825 days.

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

Authenticated sessions on the GTS platform have a maximum duration of 10 minutes.
After this period of inactivity, the session is automatically terminated, requiring a new authentication process to ensure access security and prevent unauthorized use of credentials.

6.5.1. Specific Computer Security Technical Requirements

Access to the PKI servers is restricted to the members of the Working Groups. The ROOT CA is an offline CA, only activated within the scope of periodic maintenance and deactivated immediately afterwards. The Subordinate CAs of the 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 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 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 CA. The GTS CA has mechanisms to control and monitor GTS CA 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 CA systems are in the High Security Zone (HSZ). Through the implemented controls, it is possible to guarantee the identification, authentication and administration of accesses.

For security reasons, authenticated sessions on the Global Trusted Sign platform have a maximum inactivity period of 10 minutes. After this period without any user interaction, the session is automatically terminated, and a new authentication is required to restore access to the platform.

6.6.3. Life Cycle Security Controls

The update and maintenance operations of PKI products and systems are carried out in accordance with the same security controls applicable to the initial installation. These operations are performed exclusively by members of the Global Trusted Sign Trust Groups, duly authorised, competent, and appropriately trained for this purpose, in accordance with approved internal procedures.

6.7. Network Security Controls

The Global Trusted Sign PKI has perimeter protection mechanisms, namely a firewall system, designed to protect the infrastructure against unauthorised access and other security threats.
The infrastructure implements the necessary controls in terms of identification, authentication, access control, administration, auditing, and secure information exchange. Global Trusted Sign ensures that the security controls implemented in its PKI comply with the network security requirements established by the **CA/Browser Forum – Network and Certificate System Security Requirements**, as well as all other applicable legal, regulatory, and normative requirements.

6.8. Time-Stamping

Information related to the GTS CA 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

Certificates issued by the CA follow the profile defined in ITU-T Recommendation X.509, version 3, and are issued in accordance with this Certification Practice Statement and Certification Policy, applicable legislation, and relevant technical standards.
Cryptographic keys used in the issuance and management of certificates, including Certification Authority keys, are generated, stored, and used in Qualified Signature Creation Devices (QSCD), where applicable, or in certified Hardware Security Modules (HSMs) that meet the security requirements set

out in national legislation, Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183, and applicable technical standards.

The profile of certificates issued by the GTS CA is compliant with the following reference framework:

- 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 (eIDAS), in its consolidated version, as amended by Regulation (EU) 2024/1183;
- ETSI EN 319 411-1 – *Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 1: General Requirements*;
- ETSI EN 319 411-2 – *Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing EU Qualified Certificates*;
- ETSI EN 319 412 (série) – *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles*;
- ITU-T Recommendation X.509 – *Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Framework*;
- CA/Browser Forum Baseline Requirements, where applicable to public SSL/TLS certificates.
- Detailed information about the CA GTS certificate profiles can be found at: https://pki.globaltrustedsign.com/index.html and https://pki02.globaltrustedsign.com/index.html.

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

7.1.2.1. Root CA Certificate

Information can be found in the profile of the certificates available in section 7.1 of this document, via the repositories at https://pki.globaltrustedsign.com/index.htm and https://pki02.globaltrustedsign.com/index.html, and in DP01_PL11 – ROOT GTS Certification Policy.

7.1.2.2. Subordinate CA Certificate

See section 7.1.2.1.

7.1.2.3. Subscriber Certificate

Information is available in the certificates on file, which can be consulted by accessing the https://pki.globaltrustedsign.com/ repository.

7.1.2.4. All Certificates

Information is available in the archived certificates, which can be accessed via the repositories at https://pki.globaltrustedsign.com/index.html and https://pki02.globaltrustedsign.com/index.html, as well as via PL01_GTS – Qualified Certificates Policy and PL16_GTS – Advanced Certificates 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

The requisites apply to the public key parameter field available in the certificates.

7.1.3.1. SubjectPublicKeyInfo

Information is available in the certificates on file, which can be consulted by accessing the https://pki.globaltrustedsign.com/index.html and https://pki02.globaltrustedsign.com/index.html repository and through PL01_GTS - Qualified Certificates Policy; PL16_GTS - Advanced Certificates Policy; and PL14_GTS - Timestamp Certificate Policy.

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.
Global Trusted Sign may include name constraints in the "*nameConstraints*" field when applicable.

7.1.6. Certificate Policy Object Identifier

7.1.6.1. Reserved Certificate Policy Identifiers

The certificate of the Root does not contain OID. However, the certificates issued by the GTS PKI Subordinates contain the following qualifiers: "policyQualifierID= CPS" and "cPSuri", which points to the URL where the Certification Practices Statement with the OID identified by the "policyIdentifier" is found. Other certificate policy object identifiers are included, depending on the type of certificate.
All certificates that have a policy identifier have as the following base number: 1.3.6.1.4.1.50302.

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

Not stipulated.

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

Not stipulated.

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	CN 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
    - 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

Not stipulated.

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

At the GTS CA, compliance audits shall be carried out regularly in accordance with applicable legislation by an external entity registered and recognised for this purpose, based on existing standards, and the results shall be communicated to the supervisory authority.

In accordance with Article 20(1) of Regulation (EU) No 910/2014 (eIDAS), in its consolidated version as amended by Regulation (EU) 2024/1183, EC GTS, as a qualified trust service provider, is subject to conformity audits carried out by a Conformity Assessment Body (CAB) at intervals not exceeding 24 (twenty-four) months. Without prejudice to this regular audit cycle, additional audits may be conducted on EC GTS's own initiative or at the request of the Supervisory Body, whenever deemed necessary or justified.

The documents (practice statement and certificate policies) are validated annually, according to the reference date identified in the document itself, or whenever there is a change.

8.2. Identity/Qualifications of Assessor

The Conformity Assessment Body (**CAB**) is the body defined in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008, in its consolidated version, accredited to carry out conformity assessment activities.
For the purposes of assessing Qualified Trust Service Providers (QTSPs) and the qualified trust services provided by them, the CAB shall be accredited in accordance with Regulation (EC) No 765/2008 and shall comply with the requirements laid down in Regulation (EU) No 910/2014 (eIDAS), in its consolidated version as amended by Regulation (EU) 2024/1183, as well as the applicable ETSI standards.

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 CA holders' files.

8.4. Topics Covered by Assessment

A security audit is conducted on the basis of the requirements defined in this CPS and in accordance with applicable national legislation. It aims to determine the compliance of GTS CA services with this Practice Statement and Certificate Policies. Also, it must determine the proper adequacy in relation to several documents, particularly with policies related to security, physical security, technology assessment, CA 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 CA 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.

Of the significant events generating auditable records, the following are considered:

– Security-related events, including:
    - Attempts to access (successfully and unsuccessfully) sensitive resources of the GTS CA;
    - Operations carried out by members of the Working Groups;
    - Physical security input/output devices of the various security levels.
– Requests for issuance of certificates;
– Updating of CRLs;

The entries in the records include the following information:

– Event category;
- Date and time of the event;
- Description of the event;
- Identity of the subject who caused the event;

- Serial number of the event.

Audit records are kept available for at least 1 month after processing, and then archived in accordance with national legislation.

9. Other Business and Legal Matters

- The following legal and business aspects are established and should be highlighted:
- Fees may be charged for certificate issuance and/or re-issuance processes;
- Fees may be charged for timestamping validation services;
- No fees shall be charged for the availability of certificates in the repository;
- Access to information on certificate status or Certificate Revocation Lists (CRLs) shall be free of charge, and no fees may be applied;
- No refunds are provided for certificate revocation services (see current terms and conditions FO31 and FO23).

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

The applicable fees for the issuance and re-issuance of certificates by Global Trusted Sign are published at https://globaltrustedsign.com are defined in a formal commercial proposal issued by the same.
Global Trusted Sign does not support certificate renewal processes. Whenever a certificate must be replaced, including due to the expiration of its validity period, a new issuance (re-issuance) is performed, to which the applicable fees for that service shall apply.

9.1.2. Certificate Access Fees

Not stipulated.

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 CA 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

Not stipulated.

9.2.3. Insurance or Warranty Coverage for End-Entities

Global Trusted Sign holds a civil liability insurance policy designed to provide cover for the risks arising from the provision of its qualified trust services.
The civil liability insurance is maintained in accordance with Regulation (EU) No 910/2014 (eIDAS), as consolidated and amended by Regulation (EU) 2024/1183, and Decree-Law No 12/2021 of 9 February, with Ministerial Order No. 62/2021 of 17 March, and, with regard to the issuance of Extended Validation (EV) SSL/TLS certificates, with section 8.4 of the CA/Browser Forum's Guidelines for the Issuance and Management of Extended Validation Certificates.
The insurance provides cover for civil liability for damages that may result from a breach of the legal, regulatory and contractual obligations arising from Global Trusted Sign's activities as a Qualified Trust Service Provider, in accordance with the applicable legislation and technical standards..

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

9.3.3. Responsibility to Protect Confidential Information

The GTS CA practices ensure the protection of confidentiality and integrity of the registration data, especially when transmitted between the GTS CA and the subscribers and holders, as well as during the communication between the distributed components of the GTS CA 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 CA. 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

Global Trusted Sign ensures the protection of private information processed within the scope of its trust services, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR), Law No. 58/2019 of 8 August, and other applicable national and European legislation on personal data protection and privacy.
Global Trusted Sign implements appropriate technical and organisational measures to ensure the confidentiality, integrity, availability, and resilience of personal data, ensuring that its processing is carried out lawfully, fairly, and transparently, exclusively for the authorised purposes and in strict compliance with applicable legal and regulatory obligations.

9.4.5. Notice and Consent to Use Private Information

The procedures for notification and obtaining consent for the use of private information are carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR), Law No. 58/2019 of 8 August, and other applicable national and European legislation on personal data protection.
Global Trusted Sign ensures that data subjects are duly informed about the purposes, legal bases, and conditions of processing of their private information, as well as their rights, through the Privacy Policy and other information made available at the time of data collection.
Where the processing of personal data is based on the data subject's consent, such consent is obtained freely, specifically, informedly, and unambiguously, and may be withdrawn at any time, without prejudice to the lawfulness of processing carried out prior to its withdrawal. Where the processing is based on another lawful basis under the GDPR, Global Trusted Sign ensures compliance with the respective legal requirements.

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

The conditions governing the disclosure of personal data are set out in the documents relating to the terms and conditions: FO23 – Certificate Terms and Conditions and FO31 – General Terms and Conditions.
Global Trusted Sign does not disclose personal data to third parties, except where this is necessary to comply with legal or regulatory obligations, by order of a competent authority or on another valid legal basis, in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) and other applicable legislation.

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 the GTS CA. 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

The subscriber has the right to obtain, at any time, a full copy of document FO23 – General Terms and Conditions, applicable to the provision of trust services, which constitutes the contractual agreement between the parties and governs the rights and obligations arising from the use of certificates issued by Global Trusted Sign.
In in-person validation processes, the document is issued in duplicate, with one copy provided to the subscriber and the other retained by Global Trusted Sign, duly signed by both parties, for evidentiary and archival purposes.

9.6.1. CA Representations and Warranties

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

- To conduct its operations in accordance with this 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 the present CPS;
- To publish its Practice Statement (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 CA 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 CA;
- 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 CA certificates.

9.6.2. RA Representations and Warranties

The Registration Authority (RA) is the entity responsible for analysing and evaluating the requests for GTS services, namely the veracity of the documents and validation of the identity of the holders of certificates and requests. This RA has the right to approve or reject the requests after due validation.

Additionally, the RA has the authority to approve the revocation of certificates. 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 CA prior authorization, in writing.

Subscribers have the right to request and obtain, at any time, a complete copy of document FO23 – Terms and Conditions of the Certificates, which constitutes the contractual agreement between the parties.

This document defines the responsibilities, obligations, and rights applicable to the use of certificates issued by GTS, as well as the associated service provision conditions.

9.6.4. Relying Party Representations and Warranties

Parties relying on the certificates issued by the GTS CA 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 CA in its website.

9.6.5. Representations and Warranties of other Participants

Not stipulated.

9.7. Disclaimer of Warranties

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

9.8. Limitations of Liability

The GTS CA 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 CA 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 CA does not assume any responsibility in the event of services failure related to force majeure, such as natural disasters, war or other similar.

The liability of the GTS CA is limited to damages directly resulting from its activities, namely:

a) It shall be liable for damages and losses caused to any person in the course of its activity, in accordance with Regulation (EU) No 910/2014 (eIDAS), in its consolidated version as amended by Regulation (EU) 2024/1183, and applicable national legislation.

b) It shall be liable for losses caused to the holders or to third parties due to certificate status outdated information, following a revocation or suspension of a certificate once it is aware of it.
c) It shall take responsibility over the risks that individuals may suffer as a consequence of normal, or abnormal operation of its services.
d) It is only liable for damages and losses caused by the misuse of qualified certificates where the limits regarding their intended use are not clearly defined in the certificates in a manner recognisable to third parties.
e) It shall not be responsible when the holder exceeds the limits set out in the certificate as to their possible uses, in accordance with the conditions established and communicated to the holder.
f) It shall not be liable if the recipient of electronically signed documents does not verify them and does not take into account the restrictions set out in the certificate regarding its permitted uses.
g) It assumes no liability in the event of loss or damage:
    - arising from the services provided in cases of war, natural disasters, or any other force majeure event;
    - resulting from the use of certificates beyond the limits defined therein in the Certification Practice Statement and Certification Policy;
    - caused by improper or fraudulent use of the certificates or CRL issued by it.

9.9. Indemnities

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

9.10. Term and Termination

9.10.1. Term

This CPS comes into force from the moment of its publication at the GTS CA repository and after its approval, on the terms of this document. This document 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 CA keys, when, mandatorily, a new version shall be written.

9.10.2. Termination

This CPS 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 CPS 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 CPS, related to audits, confidential information, obligations and responsibilities of GTS CA, 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 CPS must be approved by the Management Group. Amendments must be carried out through documents, containing the new amendments to the CPS.

9.12.2. Notification mechanism and period

In cases where the Management Group considers that changes to the specification may affect the acceptability of certificates for specific purposes, the corresponding certificate users shall be informed that a change has been made and that they must consult the new Certification Practice Statement and Certification Policy in the established repository. The communication mechanism shall be through:

- Website:
  - https://www.globaltrustedsign.com
- Repository:
  - https://pki.globaltrustedsign.com/index.html
  - https://pki02.globaltrustedsign.com/index.html.

9.12.3. Circumstances under which OID must be Changed

If the GTS CA determines that a change to the identifier (OID) of the CPS or certificate policy 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 CA 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 CA may be communicated to the Supervisory Authority with the purpose of the resolution of conflicts that may eventually arise.

9.14. Governing Law

The activity of ACIN – iCloud Solutions, owner of Global Trusted Sign, as a Qualified Trust Service Provider, is governed by applicable national and European legislation, namely:

- 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 (eIDAS), in its consolidated version, as amended by Regulation (EU) 2024/1183;
- Decree-Law No 12/2021 of 9 February, which ensures the implementation in national law of Regulation (EU) No 910/2014 (eIDAS);
- Ordinance No 62/2021 of 17 March, concerning civil liability insurance for Qualified Trust Service Providers;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR), and Law No 58/2019 of 8 August;
- Other applicable national and European legislation governing the provision of qualified trust service.

The QTSP also complies with the applicable technical standards and frameworks for Qualified Trust Service Providers, namely:

- ETSI EN 319 401 – *Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers*;
- ETSI EN 319 411-1 – *Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 1: General Requirements*;
- ETSI EN 319 411-2 – *Policy and Security Requirements for Trust Service Providers Issuing EU Qualified Certificates*;

- ETSI EN 319 412 (series) – *Certificate Profiles*;
- Other applicable ETSI standards and technical frameworks relevant to the trust services provided by GTS.

9.15. Compliance with Applicable Law

This document (CPS) 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 CPS 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 fully accept the content of the latest version of this Certification Practice Statement and Certification Policy. In the event that one or more provisions of this document are, or become, legally invalid, void, or unenforceable, they shall be deemed ineffective. These provisions shall only be disregarded where they are not considered essential. It is the responsibility of the Management Group to assess their essential nature. The practices adopted by the CA ensure the independence of members of the trust groups and senior management, as well as freedom from commercial, financial, or other pressures that may influence confidence in the services provided.

Additionally, it ensures that the services provided within its Public Key Infrastructure (PKI) are designed and made available in a way that allows their use by persons with disabilities, promoting accessibility, non-discrimination, and equal access to trust services, in accordance with Regulation (EU) No 910/2014 (eIDAS), in its consolidated version as amended by Regulation (EU) 2024/1183, and other applicable accessibility legislation.

9.16.2. Assignment

The parties operating under this Certification Practice Statement and Certification Policy, or applicable agreements, may not assign their rights or obligations without the prior written consent of the Global Trusted Sign Trust Group.

9.16.3. Severability

If a provision of this CPS, including limitation of liability clauses, is found to be ineffective or unenforceable, the remainder of this CPS shall be construed in the sense of the original intention of the parties. Any provision of this CPS 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)

Global Trusted Sign reserves the right to claim compensation from the responsible party for any damages, losses, costs, expenses and legal or solicitors' fees arising from a breach of the obligations set out in this Certification Practice Statement (CPS), the Terms and Conditions or applicable legislation.

The fact that Global Trusted Sign does not exercise, in whole or in part, any right or power arising from this CPS does not constitute a waiver of that right, nor does it prevent its subsequent exercise, nor does it prejudice the exercise of any other rights or powers to which it is entitled.

Any waiver of rights by Global Trusted Sign shall only be effective if it is expressly made in writing and signed by a duly authorised representative.

9.16.5. Force Majeure

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

9.17. Other Provisions

Not stipulated.