ELECTRONIC SEALS CERTIFICATE POLICY

Global Trusted Sign

Document Reference | PL02_GTS_V8
Document Classification: Public
Date: 06th may 2021

Table of Contents

1. Introduction

Purpose

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

Target Audience

This document should be read by:

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

Document Structure

It is assumed that the reader is familiar with the concepts of cryptography, public-key infrastructures and electronic signature. If this situation does not occur, it is recommended to deepen the concepts and knowledge in the topics previously mentioned before proceeding with the reading of the document. It is not intended to appoint legal rules or obligations, but rather to inform, so it is intended that this document is simple, direct and understood by a wide audience, including people without technical or legal knowledge.

1.1. Overview

The purpose of this document is to present the Electronic Seals Certificate Policy of Global Trusted Sign Certification Authority, as a qualified service provider within the framework of Regulation No. 910/2014. It is assumed that the reader is familiar with the concepts of cryptography, public-key infrastructures and electronic signature. If this situation does not occur, it is recommended to deepen the concepts and knowledge in the topics previously mentioned before proceeding with the reading of the document. The certificates issued by the GTS CA contain a reference to the GTS CA Certification Practice Statement (CPS), being the CPS supplemented by this Certificate Policy.

The respective document is elaborated with reference to the Certification Authority Practice Statement, DP02_GTS.

1.2. Document name and Identification

The certificates issued by the GTS CA contain a reference to the GTS CA Certification Practice Statement (CPS), being the CPS supplemented by this Certificate Policy.

Document information	
Document Version	8.0
Document Status	Approved
OID "Object Identifier"	1.3.6.1.4.1.50302.1.1.1.2.1.3
Issuance date	06th may 2021
Validity	06th may 2022
Location	https://pki.globaltrustedsign.com/index.html

1.2.1. Revision Record

Version Number	Creation	Approval	Reason
	06-05-2021	06-05-2021	
	Security Administration	**Group Management**	
8	Sandra Mendes y Fernández Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 06-05-2021 16:05:35	Tolentino de Deus Faria Pereira Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 06-05-2021 16:12:39	Update of document structure according to RFC 3647

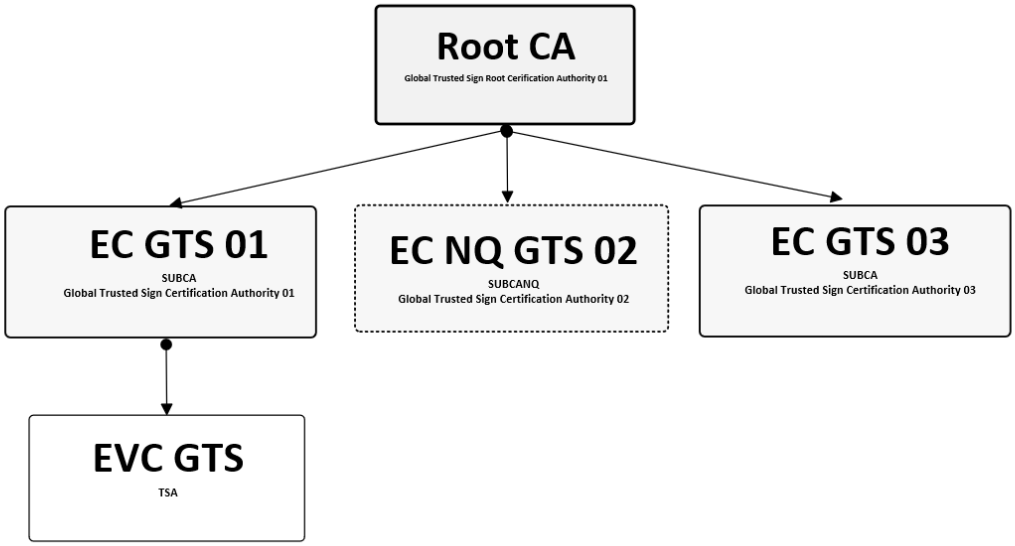
1.2.2. Relevant Dates

History of document versions

Version ID	Version Date	Reason for new version
Version 1	25-01-2018	To present the Electronic Seal Certificate Policy of the Global Trusted Sign Certification Authority
Version 2	09-02-2018	Update of certificate fields
Version 3	01-03-2018	Serial Number and Organization Identifier format update, to comply with ETSI 319 412-1
Version 4	15-03-2019	Update of document validity and OCSP
Version 5	18-05-2020	New certificate profile for signing e-mails
Version 6	02-06-2020	Addition of SUBCA 03 certificate
Version 7	23-09-2020	Update with electronic invoicing certificate profile
Version 8	06-05-2021	Update of document structure according to RFC 3647

1.3. PKI Participants

GTS, as a qualified trust service provider, has a trust hierarchy accredited by the National Security Office (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 CA01 and GTS CA03), the GTS Non-qualified Certification Authority (GTS NQ CA) and the GTS Timestamping Certification Authority (GTS TSA CA). These Certification Entities are described in sections 1.3.1.1, 1.3.1.2, 1.3.1.3 and 1.3.1.4, of this document, and are illustrated as follows:



Legend:

1 – GTS Root CA **- GTS Root Certification Authority**
2 – GTS CA 01 **– GTS Certification Authority**
3 – GTS NQ CA 02 – **GTS Non-Qualified Certification Authority**
4 – GTS TSA – GTS **- Timestamping Certification Authority**
5 – GTS CA 03 **– GTS Certification Authority**

1.4. Certificate Usage

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

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

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

1.5. Policy Administration

1.5.1. Organization Administering the Document

The management of the GTS CA Certification Practice Statement is responsibility of the GTS Trust Group.

1.5.2. Contact Entity

ACIN iCloud Solutions, Lda.
Estrada Regional 104 Nº42-A
9350-203 Ribeira Brava
Madeira – Portugal

Tel: 707 451 451 / + 351 291 957 888

https://www.globaltrustedsign.com
E-mail: info@globaltrustedsign.com

1.6. Definitions and Acronyms

1.6.1. Definitions

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

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

Definitions	
Term	**Definition**
Conformity Assessment Body	A body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides.
Public Body	National, regional or local government body, a body subject to public law or an association formed by one or more of those entities or by a body subject to public law, or a private entity authorised by, at least, one of those authorities, bodies or associations as being of public interest, under the current mandate.
Relying Party	Relying parties or final recipients are natural or legal people that trust in the validity of mechanisms and procedures used in the linking process of a time stamp to a datum. In other words, they rely on the time stamp's accuracy.
Certificate Policy	Group of rules that indicate the certificate's applicability to a specific community and/or application class with common security requirements.
Trust Service Provider	Natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
Qualified Trust Service Provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Product	Hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services.
Electronic Seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
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.

Definitions	
Term	**Definition**
Trust Service	Electronic service normally provided for remuneration which consists of: a) the creation, verification, and validation of electronic signatures, e-seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or b) the creation, verification and validation of certificates for website authentication; or c) the preservation of electronic signatures, seals or certificates related to those services.
Qualified Trust Service	Trust service that meets the applicable requirements laid down in the European Regulation 910/2014.
Electronic Registered Delivery Service	Service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.
Qualified Electronic Registered Delivery Service	Electronic registered delivery service which meets the following requirements: a) they are provided by one or more qualified trust service provider(s); b) they ensure with a high level of confidence the identification of the sender; c) they ensure the identification of the addressee before the delivery of the data; d) the sending and receiving of data is secured by an advanced electronic signature or an advanced e-seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.
Signatory	Natural person that creates an electronic signature.
Electronic Identification System	Electronic identification system under which electronic identification means are produced for natural or legal people or for natural people in representation of legal people.
Holder	See Signatory.
User	Natural or legal person that uses electronic identification or a trust service.
Validation	Process of verifying and confirming that an electronic signature or a seal is valid.
Chronological Validation	Declaration of a TSA that certifies the date and hour of creation, expedition or reception of an electronic document.
High Security Zone	Access controlled area in which an entry point is limited to authorised staff duly accredited and visitors properly accompanied. High security zones must be closed around its perimeter and watched 24 hours a day, 7 days a week, by security personnel, other personnel or by electronic means.

1.6.2. Acronyms

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

1.6.3. References

- ✓ DP02_GTS_ GTS EC Certification Practice Statement
- ✓ PC02_GTS_V5 – Electronic Seals Issuance Process
- ✓ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- ✓ ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key Certificates;
- ✓ ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, v1.2.0;
- ✓ ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, v1.1.1;
- ✓ ETSI EN 319 401 v2.1.1: General policy requirements for Trust Service Providers;
- ✓ ETSI 319 412 v1.4.2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
- ✓ RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List 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.1.7.3.

2. Publication and Repository Responsibilities

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

3. Identification and Authentication

3.1. Naming

The GTS CA ensures the issuance of certificates with a *Distinguished Name* (DN) X.509 to all holders who submit documentation in electronic format, according to what is set in RFC 5280.

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 DN:

Electronic Seal for Signature

Attribute	Code	Value
Country	C	<Holder's country>
Organization	O	<Legal name of the organisation>
Common Name	CN	<Name of the organization for which it is known>
OrganizationUnit	OU	*RemoteQSCDManagement*
Organization Identifier	OrganizationIdentifier	Unique identifier of the legal person, other than the name of the organization. (2.5.4.97) VAT format<country's code>-<TIN of the legal person> (According to 5.1.4 of the ETSI 319 412-1)

Electronic Seal for Electronic Invoicing

Attribute	Code	Value
Country	C	<Holder's country>
Organization	O	<Legal name of the organisation>
Common Name	CN	<Name of the organization for which it is known>
OrganizationUnit	OU	*RemoteQSCDManagement*
OrganizationUnit	OU	*Application certificate*
Organization Identifier	OrganizationIdentifier	Unique identifier of the legal person, other than the name of the organization. (2.5.4.97) VAT format<country's code>-<TIN of the legal person> (According to 5.1.4 of the ETSI 319 412-1)

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 DN used is appropriate for a certain holder and that the *Common Name* component of the DN represents it in a manner that can be easily identified by the interested parties.

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

3.2. Initial Identity Validation

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

Legal Person Identification

The mandatory documents submitted in the Form must enable the Registry Administrators to unambiguously validate the identity of the Applicant, namely:

- Of the natural person being represented:
    i. Given Names and Surnames (in accordance with national practice for the identification of persons)
    ii. Date and place of birth
    iii. Nationally recognised identification document that distinguishes the holder from others with the same name

iv. Document with probative value equivalent to physical presence

- Legal person:
  i. Full name and details of the legal person
  ii. Evidence of the association of the natural person with the legal person that will appear in the attributes of the certificate.

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

DNs 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.

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 and can be done in the following ways:

- In person, always with two registry administrators present in this act (paragraph a, no. 1, article 24 of Reg.910 / 2014), or;
- Remote, using electronic identification means, such as videoconferencing through certified software, for which, before the issuance of the qualified certificate, the physical presence of the natural person or an authorized representative of the legal person has been ensured; which comply with the requirements established in article 8 of Regulation 910/2014 in relation to the "substantial" or "high" guarantee levels and Resolution 154/2017 of the GNS, (paragraph b, of paragraph 1, of article 24 of Reg.910 / 2014), or
- Through a qualified electronic signature certificate or a qualified electronic seal issued under the terms of the previous paragraph (paragraph c, d, of paragraph 1, of article 24 of Reg.910/2014), only for citizens with a Portuguese identity card.

3.2.4. Non-Verified Subscriber Information

All the information provided by the subscriber is verified.

3.2.5. Validation of Authority

See section 4.

3.2.6. Criteria for Interoperation or Certification

Certificates issued on the GTS PKI are issued under a single trust hierarchy.

4. Certificate Life Cycle Operational Requirements

4.1. Certificate Application

A request to the GTS CA for the issuance of certificates begins with the completion of a form, designed for each type of certificate supported and with the acceptance of the terms and conditions established by the GTS CA, duly signed by the holder in handwritten form and which in this case implies that original documents are sent by post to GTS or in digital form, with recourse to a qualified signature.

4.1.1. Who Can Submit a Certificate Application

Certificate subscription requests may be submitted by:

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

4.1.2. Enrolment 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. GTS 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 period of 7 years, in accordance with CAB Forum section 5.5.2.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

As soon as GTS receives the certificate issuance request form, as well as the necessary information for issuing the request, it shall proceed to validate all information provided in order to verify the authenticity of the data.

4.2.2. Approval or Rejection of Certificate Applications

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

4.2.3. Time to Process Certificate Applications

GTS 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.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

This process is conducted by two Registry Administrators, through double authentication in order to verify the authenticity of data provided, depending on the type of certificate requested. Certificates are issued by interaction of the GTS CA with a cryptographic module on hardware (Hardware Secure Module - HSM), in accordance with the respective certificate policy. The public key certificate is stored in the HSM. In the case of certificates for website authentication, the certificate begins its validity at the time of issuance, and the subscriber of the certificate is notified via email, and will receive, through that channel, the public key certificate.

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.

4.5. 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

4.6.1. Circumstance for Certificate Renewal

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

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

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

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

4.6.2. Who may Request Renewal

The Subscribers/Holders of the certificates may request their renewal.

4.6.3. Processing Certificate Renewal Request

The processing of the certificate renewal request is carried out as described in point 5.6.1.

4.6.4. Notification of New Certificate Issuance to Subscriber

The subscriber of the certificate is notified via e-mail within a reasonable time after the certificate is issued, and may use any reliable mechanism to deliver the certificate to the Subscriber.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are deemed accepted after their issuance or notification of the issuance of the certificate to the Subscriber, or when there is evidence that the Subscriber has used the certificate.

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.

4.8. 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.

4.9. 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.

4.9.1. Circumstances for Revocation

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

- Cease of activities;
- Theft, loss, destruction or deterioration of the supporting device of the certificates;
- Inaccuracies in data supplied;
- Risk or suspicion of risk of the holder private key;
- Risk or suspicion of risk of the certificate access password;
- Risk or suspicion of risk of the GTS ROOT CA private keys;
- Breach of responsibilities under the CPS by the GTS ROOT CA or by the holder;
- Whenever there are credible reasons to suppose that certification services are under risk, so there are doubts about the certificate reliability;
- By legal or administrative resolution;
- Use of the certificate for abusive activities

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 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

The status of certificates issued by the GTS ROOT CA can be checked by consulting the CRL, which is issued whenever there is a revocation of the certificates issued or, in the absence of changes in the status of the certificates, on a quarterly basis. The availability in the repositories is done in a period no longer than 30 minutes, and its download is done in less than 10 seconds. In order to guarantee its availability, the CRL is released in the following repositories:

- https://pki.globaltrustedsign.com/index.html

4.9.8. Maximum Latency for CRLs

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

4.9.9. Online Revocation/Status Checking Availability

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).

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Re-Key Compromise

See 4.9.1.

4.9.13. Circumstances for Suspension

The certificate suspension process is not supported by the GTS CA.

4.10 Certificate Status Services

4.9.14. Operational Characteristics

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

4.9.15. 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.

4.11 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.

5. Management, Operational and Physical Controls

The physical security, management and operational controls and requirements are stipulated in DP02 - GTS CA Practice Statement.

6. Technical Security Controls

The technical security controls are stipulated in DP02 - GTS CA Practice Statement.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

The pair of public – private keys is associated with a holder (natural or legal person) and its main use is the digital signature. The user of the public key trusts in the respective private key, being this trust derived from the use of X.509 v3 digital certificates (linking the holder with the public key). The GTS CA digitally signs the digital certificate, ensuring that the holder has the private key (proof of holding the private key).

Certificates issued by the GTS Certification Authority:

- Have a validity limit of 1, 2 or 3 years, stated in its content.
- Are signed by the GTS Certification Authority.
- Are distributed through public systems.
- Can be stored in any type of storage units.

Security services requiring the public key of the user may need to validate the entire GTS CA chain of trust (Certificate of the GTS Certification Authority and Certificate of the GTS Root Certification Authority). These certificates are public and can be checked by any security service (https://pki.globaltrustedsign.com/index.html). The storage of keys involved in all signature processes or generation of certificates by the GTS Certification Authority are stored in a certified Hardware Security Module (HSM) which complies with the requirements set by ETSI standards. The profile of the Qualified Digital Signature certificate meets the ETSI 319 412 standards.

a) Perfil de Certificados para Selo Eletrónico

Certificate Component	Value	Type	Remarks
Version	V3	M	
Serial Number	<Assigned by the GTS Certification Authority to each certificate>	M	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	"Global Trusted Sign Certification Authority 03"		
Validity			Validity of the Certificate
Valid from	<Date of issuance>		
Valid to	<Date of issuance + 1, 2 or 3 years>		1, 2 or 3 years maximum validity
Subject		M	
Country (C)	<Country>		Nationality of the certificate's holder
OrganizationIdentifier	<Unique identifier of the legal person> (optional)	M	Unique identifier of the legal person, other than the name of the Organization. (2.5.4.97) VAT format<country's code>-<TIN of the legal person> (According to 5.1.4 of the ETSI 319 412-1)
Organization (O)	<Name of the organization>		Locality where the Organization is domiciled
Common Name (CN)	<Name of the organization for which it is known>		Name of the organization for which it is known
OrganizationUnit (OU)	*RemoteQSCDManagement*		Mandatory identifier set on the GNS Decision 155/2017
OrganizationUnit (OU)	*Application certificate*	O	Specific for electronic invoicing
Subject Alternative Name	<Email do titular>		
Subject Public Key Info		M	
Algorithm	rsaEncryption (OID: 1.2.840.113549.1.1.1)		Algorithm of the public key
subjectPublicKey	<Public Key>		Certificate's public key
Authority Key Identifier		M	
keyIdentifier	160-bit hash		It enables to identify the public key corresponding to the private key of the certificate

Certificate Component	Value	Type	Remarks
Subject Key Identifier	160-bit hash	M	Identifier of the certificate's key
Key Usage		M	
Digital Signature	"0" selected		
Non-Repudiation	"1" selected		
Key Encipherment	"0" selected		
Data Encipherment	"0" selected		
Key Agreement	"0" selected		
Key Certificate Signature	"0" selected		
CRL Signature	"0" selected		
Encipher Only	"0" selected		
Decipher Only	"0" selected		
Extended Key Usage	Email Protection (1.3.6.1.5.5.7.3.4)		
Certificate Policies		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.1.2.1.3 Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identifier and location of the GTS CA Certification Practice Statement
Basic Constraints		M	
Subject Type	End Entity		Certificate intended to End-Entities
PathLenConstraint	None		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl		Location of the GTS CA Certificate Revocation List
[2]	distributionPoint: https://pki02.globaltrustedsign.com/subca/gts_subca_crl.crl		Secondary location of the GTS CA Certificate Revocation List
Qualified Certificate Statements		M	
id-etsi-qcs-QcCompliance	*<Present extension>*		The existence of a QCStatement indicates that the certificate is qualified and issued in accordance with EU Regulation No. 910/2014
id-etsi-qcs-QcSSCD	*<Present extension>*		This parameter indicates that the private key associated to the certificate is saved on a QSCD (Qualified Signature/Seal Creation Device) in accordance with EU Regulation No. 910/2014

Certificate Component	Value	Type	Remarks
id-etsi-qcs-QcType	id-etsi-qct-QcType 2 (id-etsi-qct-eseal) Certificate for electronic seals as defined in Regulation (EU) No 910/2014		Electronic Seals Certificate as defined in the European Regulation No. 910/2014
id-etsi-qcs-QcPDS	Id-etsi-qcs-QcPDS en: https://pki.globaltrustedsign.com/index.html pt: https://pki.globaltrustedsign.com/index.html		This QCStatement has the URLs of the GTS CA Principles Disclosure Statements (PDS)
Authority Information Access		M	
[1] accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)		Certificate validation service
[1] accessLocation	http://ocsp.globaltrustedsign.com/		OCSP service location
accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parameter used to identify the GTS CA certificate and to build the chain of trust.
accessLocation	https://pki.globaltrustedsign.com/subca/gts_subca.crt		Location of the GTS CA certificate
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Algorithm used to create the signature of the certificate
Signature Value	<It contains the digital signature issued by the CA>	M	Signature of the certificate

7.1.1. Version Number

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

7.1.2. Certificate Content and Extensions; Application of RFC 5280

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

7.1.3. Algorithm Object Identifiers

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

See section 3.1.

7.1.5. Name Constraints

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

7.1.6. Certificate Policy Object Identifier

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

7.1.7. Usage of Policy Constraints Extensions

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

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

7.2. CRL Profile

7.2.1. Version Number(s)

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

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

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

- 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.