GTS ROOT CA CERTIFICATE POLICY

Global Trusted Sign

Document Reference | PL11_GTS_V8
Document Classification: Public
Date: 06th may 2021

Table of Contents

1. Introduction

Purpose

The purpose of this document is to present the Certificate Policy of the Root Certification Authority of Global Trusted Sign Certification Authority, as a qualified service provider within the framework of Regulation No. 910/2014.

Target Audience

This document should be read by:

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

1.1 Overview

The purpose of this document is to define the Policy of the GTS ROOT CA. It is not intended to appoint legal rules or obligations, but rather to inform to a general audience, in a simple and direct way, including people without technical or legal knowledge. Certificates issued by the GTS ROOT CA contain a reference to the Certification Practices Statement of the GTS ROOT CA (CPS), in order to enable relying parties and other entities or individuals interested to find information about the certificate and the policies followed by the issuing authority.

This document has been elaborated with reference to the GTS Root CA Certification Practice Statement, DP01_GTS.

1.2 Document name and Identification

The present document is the GTS ROOT CA Certificate Policy, hereinafter referred to as CP. The CP is represented in a certificate through a unique number designated as "object identifier" (OID). This document is identified by the data contained in the following table:

Document information	
Document Version	8.0
Document Status	Approved
OID **"Object Identifier"**	1.3.6.1.4.1.50302.1.1.2.1.1.0
Issuance date	06th may 2021
Validity	06th may 2021
Location	https://pki.globaltrustedsign.com/index.html

1.2.1. Revision Record

Version Number	Creation	Approval	Reason
	06-05-2021	**06-05-2021**	
08	**Security Administration**	**Group Management**	Update of document structure according to RFC 3647
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 06-05-2021 16:29:11	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 06-05-2021 16:30:29	

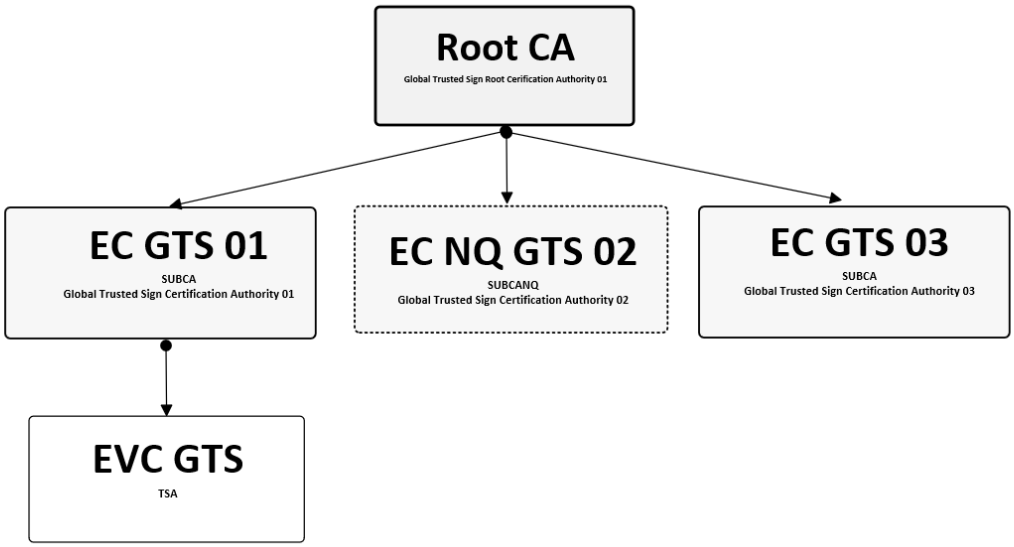
1.2.2. Relevant Dates

History of document versions

Version ID	Version Date	Reason for new version
Version 1	31-07-2017	To present the Certificate Policy of the Root Certification Authority of Global Trusted Sign, as a qualified service provider under regulation 910/2014
Version 2	15-01-2018	QtimeStamp change - ETSI EN 319 421
Version 3	31-01-2019	Annual verification, Change of key usage. TSA certificate update
Version 4	13-12-2019	Update with specific certificate for physicians
Version 5	06-03-2020	Update of the TSP Architecture
Version 6	24-06-2020	Addition of SUBCA 03 certificate
Version 7	17-09-2020	Update of registration of employees of the GTS Trust Group
Version 8	06-05-2021	Update of document structure according to RFC 3647

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.
Validation Data	Data that is used to validate an electronic signature or an e-seal.

Definitions	
Term	**Definition**
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.
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.

Definitions	
Term	**Definition**
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.
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.

Definitions	
Term	**Definition**
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

- ✓ DP01_GTS - GTS Root CA Certification Practice Statement
- ✓ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- ✓ ETSI 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 319 412 v1.4.2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
- ✓ ETSI EN 319 401 v2.1.1: Electronic Signatures and Infrastructures (ESI); 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.1.7.4.

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 allocation of names follows the convention established in the Certification Practice Statement.

3.1.1 Types of Names

The GTS ROOT CA certificate is identified by a Distinguished Name (DN), according to what is set in RFC 5280.

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

3.1.2 Need for Names to be Meaningful

The GTS 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

3.2.1 Method to Prove Possession of Private Key

In the self-signed GTS ROOT CA certificate, proof of possession of the private key shall be guaranteed through the physical presence of the various relevant Working Groups in the ceremony for issuing this type of certificates. In this ceremony, the certificate request shall be generated and presented in PKCS#10 format, whose signature on the public key information shall be validated.

3.2.2 Authentication of Organization and Domain Entity

No stipulation.

3.2.3 Authentication of Individual Identity

No stipulation.

3.2.4 Non-Verified Subscriber Information

All the information provided by the subscriber is verified.

3.2.5 Validation of Authority

No stipulation.

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

4.1.1 Who Can Submit a Certificate Application

Only the ACIN ICloud Solutions, Lda. administration can submit an application for a GTS ROOT CA self-signed certificate.

4.1.2 Enrolment Process and Responsibilities

The certificate registration process consists of the following steps, to be carried out by the GTS Trust Groups:

- Generation of the public and private key pairs in the appropriate cryptographic environment;
- Generation of the corresponding PKCS#10 in the appropriate cryptographic environment.

4.2 Certificate Application Processing

The certificate request is processed as follows:

- Creation of the key pair and signing of the certificate in the appropriate cryptographic environment according to the profile indicated in this policy;
- Certificate availability.

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.

4.2.3. Time to Process Certificate Applications

After approval of the certificate request, the certificate should be issued within ten business days.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The certificate issuance process is conducted by the Registry Administrators in the GTS ROOT CA, through a specific ceremony for that purpose. The certificates are issued through the interaction of the GTS ROOT CA with a cryptographic module in hardware (Hardware Secure Module - HSM). The issued certificate begins its validity at the time of its issuance.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The certificate is issued in person, according to the previous section.

4.3.3 Conduct Constituting Certificate Acceptance

The conclusion of the certificate issuance ceremony implies formal acceptance by the GTS representatives of the functionalities and content of the certificate, as well as the rights and responsibilities.

4.3.4 Publication of the Certificate by the CA

The GTS ROOT CA does not publish certificates issued.

4.3.5 Notification of Certificate Issuance by the CA to other Entities

The GTS ROOT CA does not notify other entities of the issuance of certificates.

4.4 Key Pair and Certificate Usage

4.4.1 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 if applicable for the type of certificate in question:

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 the GTS ROOT CA.

4.4.2 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, suspended or revoked. The GTS ROOT CA supplies in this CPS information about the appropriate services available to verify the validity status of the certificate, such as OCSP and CRL.

4.5 Certificate Renewal with Generation of a New Key Pair

In the GTS ROOT CA, there is no certificate renewal process, with the holder being obligated to make a new certificate issuance application with the same parameters. This process requires the generation of a new key pair, and respective certificate. The renewal of certificates uses the authentication and initial identification procedures that result in the generation of new key pairs.

4.5.1 Circumstances for Certificate Renewal with Generation of a New Key Pair

No stipulation.

4.5.2 Who may Request Certificate Renewal with Generation of a New Key Pair

No stipulation.

4.5.3 Processing Certificate Renewal with Generation of a New Key Pair

No stipulation.

4.5.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.5.5 Conduct Constituting Acceptance of a Renewal Certificate with Generation of a New Key Pair

No stipulation.

4.5.6 Publication of the Renewal Certificate with Generation of a New Key Pair by the CA

No stipulation.

4.5.7 Notification of Certificate Renewal with Generation of a New Key Pair by the CA to Other Entities

No stipulation.

4.6 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 ROOT CA.

4.6.1 Circumstances for Suspension

No stipulation.

4.6.2 Who can Request Suspension

No stipulation.

4.6.3 Procedure for Suspension Request

No stipulation.

4.6.4 Suspension Period

No stipulation.

4.6.5 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.

4.6.6 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.

4.6.7 Procedure for Revocation Request

The revocation requests of the GTS ROOT CA self-signed certificate shall be addressed in writing or through an electronic message digitally signed by the Administration of Acin iCloud Solutions, Lda. The entity is then identified and the respective request is registered and filed. After analysis by the GTS management group, the same shall provide the necessary information for the respective revocation to the other working groups. In any case, a detailed description of the entire decision process is filed and documented:

- Date of the revocation request
- Name of the certificate holder
- Detailed description of the reasons for the revocation request
- Name and functions of the person that requests the revocation
- Contact information of the person that requests the revocation;
- Signature of the person that requests the revocation request.

4.6.8 Effectiveness of Revocation

The revocation will be made immediately after all the procedures referred to in the previous point have been completed.

4.6.9 Time within which CA must Process the Revocation Request

The revocation request must be processed immediately, and in no case longer than 24 hours.

4.6.10 Revocation Checking Requirement for Relying Parties

Before using a certificate, the relying parties have as their responsibility to verify the status of all the certificates, through the CRLs or a verification server of the online status (via OCSP).

4.6.11 CRL Issuance Frequency

The GTS ROOT CA provides the CRLs on a quarterly basis.

4.6.12 Maximum Period between Issuance and Publication of the CRL

The maximum period between issuance and publication of the CRL shall not exceed 30 minutes.

4.6.13 Online Revocation/Status Checking Availability

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

4.6.14 Online Revocation Checking Requirements

Before using a certificate, the relying parties have as their responsibility to verify the status of all the certificates, through the CRLs or a verification server of the online status (via OCSP). CRLs can be accessed at https://pki.globaltrustedsign.com/index.html, guaranteeing their availability 24 hours a day, 7 days a week, except in the occurrence of some scheduled maintenance stoppage and duly communicated to the parties involved. The end of the subscription of a certificate occurs when the validity period is exceeded, expired or the certificate is revoked, according to RFC 3647.

4.7 Certificate and Key Pair Usage by the Subscriber

The GTS ROOT CA is the holder of the self-signed Global Trusted Sign Root Certification Authority 01 certificate. This certificate is used to sign the subordinate certification authorities that belong to the hierarchy of the GTS ROOT CA, as well as the Certificate Revocation List itself, under the terms defined in the Certification Practices Statement.

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

The GTS ROOT CA certificate profile is in accordance with a set of standards:

- 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 EN 319 401 – General Policy Requirements for Trust Service Providers, and standards related to the qualified trust services;
- ITU.T X.5099 Recommendation;
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates.

7.1. Profile of the GTS ROOT CA Self-Signed Certificate

Certificate Component	Value	Type	Remarks
Version	V3	M	
Serial Number	<Assigned by the GTS Certification Authority to each certificate>	M	Unique identifier of the certificate
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Certificate signature
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Root Certification Authority 01		
Validity		M	Validity of the Certificate
Valid from	<Date of issuance>		01/07/2017
Valid to	<Date of issuance + 20 years>		Maximum validity of 20 years
Subject		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	<Fully Qualified Domain Name of the Certification Authority>		
Subject Public Key Info		M	
Algorithm	rsaEncryption (OID: 1.2.840.113549.1.1.1)		Public key algorithm
subjectPublicKey	<Public Key>		Certificate public key
Authority Key Identifier		M	
keyID	160-bit hash		It allows to identify the public key corresponding to the private key of the certificate
Subject Key Identifier	160-bit hash	M	Certificate key identifier
Key Usage		M	
Digital Signature	"0" selected		
Non-Repudiation	"0" selected		
Key Encipherment	"0" selected		
Data Encipherment	"0" selected		
Key Agreement	"0" selected		
Key Certificate Signature	"1" selected		

CRL Signature	"1" selected		
Off-line CRL Signing	"1" selected		
Encipher Only	"0" selected		
Decipher Only	"0" selected		
Basic Constraints		M	
Subject Type	CA		Certificate intended to End-Entities
PathLenConstraint	None		
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Algorithm used to create the certificate signature.
Signature Value	<It contains the digital signature issued by the CA>	M	Certificate signature

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

The "*certificate policies*" extension is not active in the GTS ROOT CA self-signed certificate.

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.