GTS ROOT CA CERTIFICATION PRACTICE STATEMENT AND CERTIFICATION POLICY

Global Trusted Sign

Document Reference | DP01_PL11_GTS

Document Classification: Public

Date: 7 July 2026

Document OID:

- Practice Statement - 1.3.6.1.4.1.50302.1.1.1.2.1.2
- Disclosure of Principles - 1.3.6.1.4.1.50302.1.1.3.1.1.0
- Policy - 1.3.6.1.4.1.50302.1.1.2.1.1.0

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.
17	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 8

1.1 OVERVIEW 8
1.2 DOCUMENT NAME AND IDENTIFICATION 9
1.2.1 Revisions 9
1.2.2 Relevant Dates 9
1.3 PKI PARTICIPANTS 10
1.3.1 Certification Authorities 10
1.3.2 Registration Authorities 16
1.3.3 Subscribers 16
1.3.4 Relying Parties 17
1.3.5 Other Participants 17
1.4 CERTIFICATE USAGE 18
1.4.1 Appropriate Certificate Uses 19
1.4.2 Prohibited Certificate Uses 19
1.5 POLICY ADMINISTRATION 19
1.5.1 Organisation Administering the Document 19
1.5.2 Contact Person 19
1.5.3 Person Determining CPS suitability for the policy 20
1.5.4 Document approval procedures 20
1.6 DEFINITIONS AND ACRONYMS 21
1.6.1 Definitions 21
1.6.2 Acronyms 26
1.6.3 References 27
1.6.4 Conventions 27

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 27

2.1 REPOSITORIES 27
2.2 PUBLICATION OF INFORMATION 28
2.3 TIME OR FREQUENCY OF PUBLICATION 28
2.4 ACCESS CONTROLS ON REPOSITORIES 29

3 IDENTIFICATION AND AUTHENTICATION 29

3.1 NAMING 29
3.1.1 Types of names 29
3.1.2 Need for names to be meaningful 30
3.1.3 Anonymity or pseudonymity of subscribers 30
3.1.4 Rules for interpreting various name forms 31
3.1.5 Uniqueness of names 31
3.1.6 Recognition, authentication, and role of trademarks 31
3.2 INITIAL IDENTITY VALIDATION 31
3.2.1 Method to prove possession of private key 32
3.2.2 Authentication of Organisation and Domain Identity 32
3.2.2.1 Identity 33
3.2.2.2 DBA/Tradename 34
3.2.2.3 Verification of Country 34
3.2.2.4 Validation of Domain Authorisation or Control 34
3.2.2.5 Authentication for an IP Address 34
3.2.2.6 Wildcard Domain Validation 34
3.2.2.7 Data Source Accuracy 34
3.2.2.8 CAA Records 35
3.2.3 Authentication of individual identity 35
3.2.4 Non-verified subscriber information 38

3.2.5 Validation of authority *38*
3.2.6 Criteria for Interoperation or Certification *38*
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 39
3.3.1 Identification and authentication for routine re-key *39*
3.3.2 Identification and authentication for re-key after revocation *39*
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 39

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 40

4.1 CERTIFICATE APPLICATION 40
4.1.1 Who can submit a certificate application *40*
4.1.2 Enrollment process and responsibilities *40*
4.2 CERTIFICATE APPLICATION PROCESSING 41
4.2.1 Performing identification and authentication functions *41*
4.2.2 Approval or rejection of certificate applications *41*
4.2.3 Time to process certificate applications *42*
4.3 CERTIFICATE ISSUANCE 42
4.3.1 CA actions during certificate issuance *42*
4.3.2 Notification to subscriber by the CA of issuance of certificate *42*
4.4 CERTIFICATE ACCEPTANCE 42
4.4.1 Conduct constituting certificate acceptance *42*
4.4.2 Publication of the certificate by the CA *43*
4.4.3 Notification of certificate issuance by the CA to other entities *43*
4.5 KEY PAIR AND CERTIFICATE USAGE 43
4.5.1 Subscriber private key and certificate usage *43*
4.5.2 Relying party public key and certificate usage *43*
4.6 CERTIFICATE RENEWAL 44
4.6.1 Circumstance for certificate renewal *44*
4.6.2 Who may request renewal *44*
4.6.3 Processing certificate renewal requests *44*
4.6.4 Notification of new certificate issuance to subscriber *44*
4.6.5 Conduct constituting acceptance of a renewal certificate *44*
4.6.6 Publication of the renewal certificate by the CA *45*
4.6.7 Notification of certificate issuance by the CA to other entities *45*
4.7 CERTIFICATE RE-KEY 45
4.7.1 Circumstance for certificate re-key *45*
4.7.2 Who may request certification of a new public key *45*
4.7.3 Processing certificate re-keying requests *45*
4.7.4 Notification of new certificate issuance to subscriber *45*
4.7.5 Conduct constituting acceptance of a re-keyed certificate *45*
4.7.6 Publication of the re-keyed certificate by the CA *45*
4.7.7 Notification of certificate issuance by the CA to other entities *46*
4.8 CERTIFICATE MODIFICATION 46
4.8.1 Circumstance for certificate modification *46*
4.8.2 Who may request certificate modification *46*
4.8.3 Processing certificate modification requests *46*
4.8.4 Notification of new certificate issuance to subscriber *46*
4.8.5 Conduct constituting acceptance of modified certificate *46*
4.8.6 Publication of the modified certificate by the CA *46*
4.8.7 Notification of certificate issuance by the CA to other entities *47*
4.9 CERTIFICATE REVOCATION AND SUSPENSION 47
4.9.1 Circumstances for revocation *47*
4.9.1.1 Reasons for Revoking a Subscriber Certificate 47
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate 49
4.9.2 Who can request revocation *49*
4.9.3 Procedure for revocation request *50*

4.9.4 Revocation request grace period *50*
4.9.5 Time within which CA must process the revocation request *51*
4.9.6 Revocation checking requirement for relying parties *51*
4.9.7 CRL issuance frequency (if applicable) *51*
4.9.8 Maximum latency for CRLs (if applicable) *51*
4.9.9 On-line revocation/status checking availability *51*
4.9.10 On-line revocation checking requirements *52*
4.9.11 Other forms of revocation advertisements available *52*
4.9.12 Special requirements re key compromise *52*
4.9.13 Circumstances for suspension *52*
4.9.14 Who can request suspension *52*
4.9.15 Procedure for suspension request *52*
4.9.16 Limits on suspension period *53*
4.10 CERTIFICATE STATUS SERVICES 53
4.10.1 Operational characteristics *53*
4.10.2 Service availability *53*
4.10.3 Optional features *53*
4.11 END OF SUBSCRIPTION 53
4.12 KEY ESCROW AND RECOVERY 53
4.12.1 Key escrow and recovery policy and practices *53*
4.12.2 Session key encapsulation and recovery policy and practices *54*

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS 54

5.1 PHYSICAL SECURITY CONTROLS 54
5.1.1 Site location and construction *54*
5.1.2 Physical access *54*
5.1.3 Power and air conditioning *55*
5.1.4 Water exposures *56*
5.1.5 Fire prevention and protection *56*
5.1.6 Media storage *56*
5.1.7 Waste disposal *56*
5.1.8 Off-site backup *57*
5.2 PROCEDURAL CONTROLS 57
5.2.1 Trusted roles *57*
5.2.2 Number of Individuals Required per Task *59*
5.2.3 Identification and authentication for each role *59*
5.2.4 Roles requiring separation of duties *60*
5.3 PERSONNEL CONTROLS 60
5.3.1 Qualifications, experience, and clearance requirements *60*
5.3.2 Background check procedures *60*
5.3.3 Training Requirements and Procedures *61*
5.3.4 Retraining frequency and requirements *61*
5.3.5 Job rotation frequency and sequence *61*
5.3.6 Sanctions for unauthorised actions *61*
5.3.7 Independent Contractor Controls *62*
5.3.8 Documentation supplied to personnel *62*
5.4 AUDIT LOGGING PROCEDURES 62
5.4.1 Types of events recorded *62*
5.4.2 Frequency of processing audit log *63*
5.4.3 Retention period for audit log *63*
5.4.4 Protection of audit log *63*
5.4.5 Audit log backup procedures *63*
5.4.6 Audit collection System (internal vs. external) *63*
5.4.7 Notification to event-causing subject *64*
5.4.8 Vulnerability assessments *64*

5.5 RECORDS ARCHIVAL 64
5.5.1 Types of records archived *64*
5.5.2 Retention period for archive *65*
5.5.3 Protection of archive *65*
5.5.4 Archive backup procedures *65*
5.5.5 Requirements for time-stamping of records *65*
5.5.6 Archive collection system (internal or external) *65*
5.5.7 Procedures to obtain and verify archive information *65*
5.6 KEY CHANGEOVER 65
5.7 COMPROMISE AND DISASTER RECOVERY 66
5.7.1 Incident and compromise handling procedures *66*
5.7.2 Recovery Procedures if Computing resources, software, and/or data are corrupted *66*
5.7.3 Recovery Procedures after Key Compromise *67*
5.7.4 Business continuity capabilities after a disaster *67*
5.8 CA OR RA TERMINATION 67

6 TECHNICAL SECURITY CONTROLS 68

6.1 KEY PAIR GENERATION AND INSTALLATION 68
6.1.1 Key pair generation *68*
6.1.1.1 CA Key Pair Generation 68
6.1.1.2 RA Key Pair Generation 68
6.1.1.3 Subscriber Key Pair Generation 68
6.1.2 Subscriber Key Pair Generation *69*
6.1.3 Public key delivery to certificate issuer *69*
6.1.4 CA public key delivery to relying parties *69*
6.1.5 Key sizes *69*
6.1.6 Public key parameters generation and quality checking *69*
6.1.7 Key usage purposes (as per X.509 v3 key usage field) *69*
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 70
6.2.1 Cryptographic module standards and controls *70*
6.2.2 Private key (n out of m) multi-person control *70*
6.2.3 Private key escrow *70*
6.2.4 Private key backup *71*
6.2.5 Private key archival *71*
6.2.6 Private key transfer into or from a cryptographic module *71*
6.2.7 Private key storage on cryptographic module *71*
6.2.8 Activating Private Keys *71*
6.2.9 Deactivating Private Keys *71*
6.2.10 Destroying Private Keys *72*
6.2.11 Cryptographic Module Rating *72*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 72
6.3.1 Public key archival *72*
6.3.2 Certificate operational periods and key pair usage periods *72*
6.4 ACTIVATION DATA 72
6.4.1 Activation data generation and installation *72*
6.4.2 Activation data protection *73*
6.4.3 Other aspects of activation data *73*
6.5 COMPUTER SECURITY CONTROLS 73
6.5.1 Specific computer security technical requirements *73*
6.5.2 Computer security rating *73*
6.6 LIFE CYCLE TECHNICAL CONTROLS 73
6.6.1 System development controls *73*
6.6.2 Security management controls *74*
6.6.3 Life cycle security controls *74*
6.7 NETWORK SECURITY CONTROLS 74

6.8 TIME-STAMPING 74

7 CERTIFICATE, CRL, AND OCSP PROFILES 74

7.1 CERTIFICATE PROFILE 75
7.1.1 Version number(s) 85
7.1.2 Certificate Content and Extensions; Application of RFC 5280 86
7.1.2.1 Root CA certificate 86
7.1.2.2 Subordinate CA certificate 86
7.1.2.3 Certificate subscribers 86
7.1.2.4 All certificates 86
7.1.2.5 Applicability of RFC 5280 86
7.1.3 Algorithm object identifiers 86
7.1.3.1 SubjectPublicKeyInfo 86
7.1.3.2 Signature AlgorithmIdentifier 86
7.1.4 Name Forms 87
7.1.4.1 Name encoding 87
7.1.4.2 Subject information - Subscriber certificates 87
7.1.4.3 Subject information - Root certificates and subordinate CA certificates 87
7.1.5 Name constraints 87
7.1.6 Certificate policy object identifier 87
7.1.6.1 Reserved Certificate Policy Identifiers 87
7.1.6.2 Root CA certificates 87
7.1.6.3 Subordinate CA certificates 87
7.1.6.4 Subscriber certificates 88
7.1.7 Usage of Policy Constraints extension 88
7.1.8 Policy qualifiers syntax and semantics 88
7.1.9 Processing semantics for the critical Certificate Policies extension 88
7.2 CRL PROFILE 88
7.2.1 Version number(s) 88
7.2.2 CRL and CRL entry extensions 89
7.3 OCSP PROFILE 89
7.3.1 Version number(s) 89
7.3.2 OCSP extensions 89

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 89

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 89
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 90
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 90
8.4 TOPICS COVERED BY ASSESSMENT 90
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 90
8.6 COMMUNICATION OF RESULTS 91
8.7 SELF-AUDITS 91

9 OTHER BUSINESS AND LEGAL MATTERS 92

9.1 FEES 92
9.1.1 Certificate issuance or renewal fees 92
9.1.2 Certificate access fees 92
9.1.3 Revocation or status information access fees 92
9.1.4 Fees for other services 92
9.1.5 Refund policy 93
9.2 FINANCIAL RESPONSIBILITY 93
9.2.1 Insurance coverage 93
9.2.2 Other assets 93
9.2.3 Insurance or warranty coverage for end-entities 93

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 93
9.3.1 Scope of confidential information 93
9.3.2 Information not within the scope of confidential information 94
9.3.3 Responsibility to protect confidential information 94
9.4 PRIVACY OF PERSONAL INFORMATION 94
9.4.1 Privacy plan 94
9.4.2 Information treated as private 94
9.4.3 Information not deemed private 95
9.4.4 Responsibility to protect private information 95
9.4.5 Notice and consent to use private information 95
9.4.6 Disclosure pursuant to judicial or administrative process 95
9.4.7 Other information disclosure circumstances 96
9.5 INTELLECTUAL PROPERTY RIGHTS 96
9.6 REPRESENTATIONS AND WARRANTIES 96
9.6.1 CA representations and warranties 96
9.6.2 RA representations and warranties 97
9.6.3 Subscriber representations and warranties 98
9.6.4 Relying party representations and warranties 98
9.6.5 Representations and warranties of other participants 98
9.7 DISCLAIMERS OF WARRANTIES 98
9.8 LIMITATIONS OF LIABILITY 98
9.9 INDEMNITIES 99
9.10 TERM AND TERMINATION 99
9.10.1 Term 99
9.10.2 Termination 99
9.10.3 Effect of termination and survival 100
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 100
9.12 AMENDMENTS 100
9.12.1 Procedure for amendment 100
9.12.2 Notification mechanism and period 100
9.12.3 Circumstances under which OID must be changed 101
9.13 DISPUTE RESOLUTION PROVISIONS 101
9.14 GOVERNING LAW 101
9.15 COMPLIANCE WITH APPLICABLE LAW 102
9.16 MISCELLANEOUS PROVISIONS 102
9.16.1 Entire agreement 102
9.16.2 Assignment 103
9.16.3 Severability 103
9.16.4 Enforcement (attorneys' fees and waiver of rights) 103
9.16.5 Force Majeure 103
9.17 OTHER PROVISIONS 103

1 INTRODUCTION

a) Scope

The purpose of this document is to present the Certification Policy, as well as the Practices Statement that specifies the policies and procedures of the Root Certification Authority of Global Trusted Sign, hereinafter referred to as the 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 standards, in support of its activity of issuing qualified and advanced certificates of the Global Trusted Sign Root Certification Authority, hereinafter referred to as the ROOT CA.

b) Target Audience

This document is publicly available and can be read by:

- Human resources assigned to the CA working groups;
- Third parties in charge of auditing the CA;
- All participants related to the Root Certification Authority;
- All the general public

c) Document structure

This document follows the structure defined 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 document.

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

1.1 Overview

The purpose of this document is to define the GTS ROOT CA Certification Practice Statement and Certification Policy. It is not intended to name legal rules or obligations, but rather to inform, so this document is intended to be simple, straightforward and understood by a wide audience, including people without technical or legal knowledge. Certificates issued by the GTS ROOT CA contain a

reference to the GTS ROOT CA Certification Practice Statement so that relying parties and other interested entities or persons can find information about the certificate and the policies followed by the entity that issued it.

The practices of creating, signing and issuing certificates, as well as revoking invalid certificates, carried out by a Certification Authority (CA) are fundamental to guaranteeing the reliability and trust of a Public Key Infrastructure (PKI). This document 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 the lifecycle management of qualified certificates in accordance with existing certificate policies.

1.2 Document name and identification

1.2.1 Revisions

This document is called "GTS ROOT CA Certification Practice Statement and Certification Policy", the information on which is as follows:

Document information	
Document Name	GTS ROOT CA Certification Practice Statement and Certification Policy
Document Version	17
Document Status	Approved
OID	• Practice Statement - 1.3.6.1.4.1.50302.1.1.1.2.1.2 • Disclosure of Principles - 1.3.6.1.4.1.50302.1.1.3.1.1.0 • Policy - 1.3.6.1.4.1.50302.1.1.2.1.1.0
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 new version
Version 1	31-07-2017	ROOT CA GTS Certification Practices Statement
Version 2	12-09-2017	Content update
Version 3	15-01-2018	QtimeStamp - ETSI EN 319 421
Version 4	05-03-2018	Updated formatting and general content
Version 5	01-06-2018	Update of points: 9.1.3., 13.8 and 16.2
Version 6	01-04-2019	Update of Practices according to CAB forum 1.6.3

Version 7	02-05-2020	Updating the GTS CA hierarchy
Version 8	24-06-2020	Updating the GTS CA hierarchy with SUBCA 03
Version 9	23-09-2020	Update of GTS Trust Group employee records
Version 10	06-05-2021	Document structure update in accordance with RFC 3647
Version 11	23-06-2021	General content update
Version 12	19-07-2022	Annual validation of the document
Version 13	15-02-2023	Update of the PKI hierarchy and structural revision of the document
Version 14	04-07-2023	Annual verification of the document and updating of the values associated with telephone contacts
Version 15	05-09-2024	Annual review of the document and merger with PL11 and DP05
Version 16	09-09-2025	Annual review of the document
Version 17	07-07-2026	Annual review of the document, including the correction of DN references to CN, updating of identity validation proce sses, strengthening of subscribers' rights, and updating of the platform's registration and security requirements.

1.3 PKI Participants

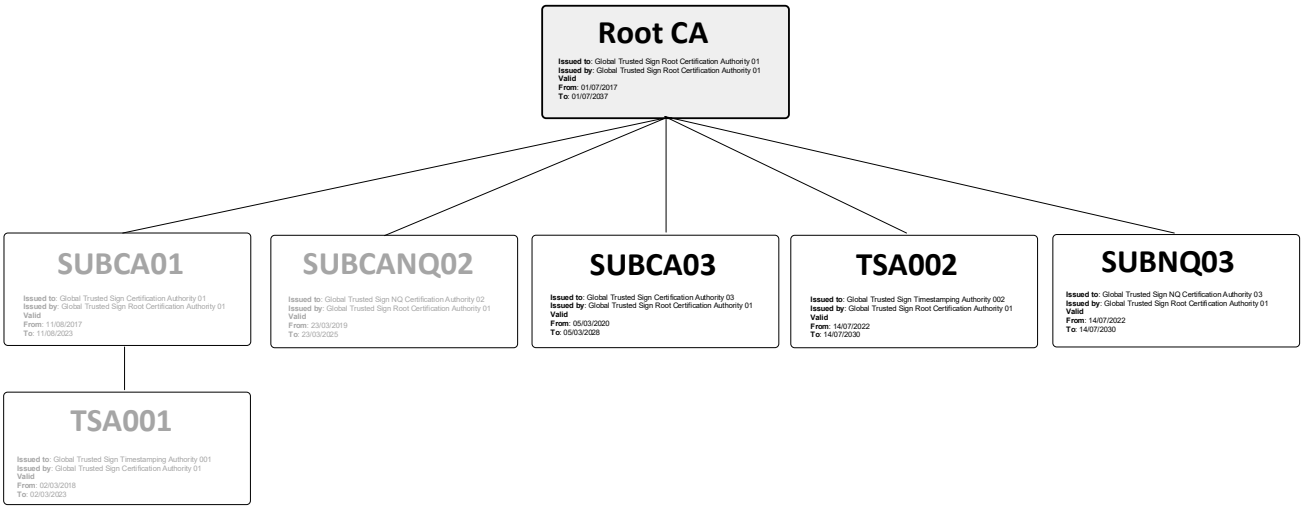
1.3.1 Certification Authorities

ACIN-iCloud Solutions, acts as the Certification Authority, with the following corporate data:
Social denomination: ACIN-iCloud Solutions, Lda.
TIN: 511 135 610
Address: Estrada Regional 104, N.º 42 A, 9350-203 Ribeira Brava. Portugal.
Phone Number: Local: 707 451 451 [1]/ International +351 291 957 888[2]
Website: 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

[1] Maximum price per minute: 0.09€ (+VAT) for calls originating on fixed networks and 0.13€ (+VAT) for calls originating on mobile networks;
[2] Cost of an international call to a fixed network, according to the tariff in force.

certificates described in this document. The GTS trust hierarchy is composed by the GTS Root Certification Authority (GTS ROOT CA), the GTS Certification Authorities (GTS CA 01 – SUBCA01 and GTS CA 03 – SUBCA03), the GTS Non-Qualified Certification Authority (GTS NQ CA – SUBCANQ02 and SUBNQ03) and the GTS Time Stamps Certification Authority (GTS TSA GTS – TSA001 and TSA002).



Legend:

1 – GTS ROOT CA – GTS Root Certification Authority

2 – SUBCA01 - Certification Authority

3 – TSA001 - GTS Timestamping Certification Authority

4 – SUBCANQ02 - GTS Non-Qualified Certification Authority

5 – SUBCA03– GTS Certification Authority

6 – TSA002 – GTS Timestamping Certification Authority

7 – SUBNQ03 – GTS Non-Qualified Certification Authority

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 signatures**

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 Authorities

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 FO31_GTS - General Terms and Conditions.

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.

1.4.1 Appropriate Certificate Uses

The requirements and rules defined in this document apply to all certificates issued by the GTS ROOT CA and will be used in accordance with the function and purpose established herein and in the corresponding Certificate Policies, in accordance with the law in force. Relying Parties can verify the chain of trust of a certificate issued by the GTS ROOT CA, thus guaranteeing the authenticity and identity of the holder.

1.4.2 Prohibited Certificate Uses

Certificates issued in the GTS ROOT 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 ROOT 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.

1.5 Policy administration

1.5.1 Organisation Administering the Document

The Global Trusted Sign Trust Group is responsible for managing this ROOT CA Certification Practice Statement and Certification Policy.

1.5.2 Contact Person

Name	GTS Trust 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
Website	https://www.globaltrustedsign.com
Phone Number	National: 707 451 451[1] International: + 351 291 957 888[2] (GTS - Option 3) [1] Maximum price per minute: 0.09€ (+VAT) for calls originating on fixed networks and 0.13€ (+VAT) for calls originating on mobile networks; [2] Cost of an international call to a fixed network, according to the tariff in force.

Whenever any of the grounds for revocation set out in section 4.9.1 are identified, they should be communicated to the above-mentioned contacts or preferably to the reporting e-mail address.

1.5.3 Person Determining CPS suitability for the policy

The Practice Statement and Certification Policy 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 ROOT CA Management Group, for its approval.

1.5.4 Document approval procedures

The validation of this document and all corrections or updates are performed by GTS Security Administration. All corrections or updates are published in the form of new versions of this Practice Statement and Certification Policy, replacing any previously defined. The GTS Security Administration is responsible for determining when changes to the Practice Statement and Certification Policy will result in a change on the object identifiers (OID) of the respective Certification Policies and Statements. After validation, the Practice Statement and Certification Policy 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 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, 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) 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
DPC	Certification Practice Statement
DR	Regulatory Decree
EC	Certification Authority
ER	Registry Authority
GNS	National Security Office (*Gabinete Nacional de Segurança*)
GTS	Global Trusted Sign
HSM	Hardware Secure Module
LRC	Certificate Revocation List
O	Organisation
OU	Organisation Unit
OID	Object Identifier
PC	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 ROOT 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 ROOT CA conducts the following publications, with the following frequency of publication:

- The GTS ROOT CA certificate is published after its issuance;
- The CRL is published quarterly;
- New versions or amendments to the respective Practice Statement and Certification Policy will be 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 ROOT CA ensures the issuance of certificates with a Common 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.

The assignment of names fulfils the requirements specified in the certificate policies for each type of profile presented.

3.1.1 Types of names

The GTS ROOT CA certificate is identified by a unique name (CN – Common Name) according to the X.500 standard.

The various types of certificates can contain the following fields in the CN:

Attribute	Code	Rules
Country	C	Country code of the certificate holder
Organisation	O	This field corresponds to the organisation (or equivalent) to which the certificate holder belongs.
Organisation Unit	OU	This field corresponds to information on the organisational unit (or equivalent) to which the certificate holder belongs.
Common Name	CN	Unique name of the certificate holder. In the case of website servers, this will be designated by the FQDN (CN = "FQDN".); designation by IP address is prohibited. In the case of qualified signature certificates, it contains the holder's name or pseudonym. In the case of electronic seal certificates, it contains the name of the legal person.
Serial Number	serialNumber	It follows the recommendations of ETSI EN 319 412.

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

Attribute	Code	Value
Common Name	CN	CN = Global Trusted Sign Root Certification Authority 01
Organisation Unit	OU	OU = Global Trusted Sign
Organisation	O	O = ACIN-iCloud Solutions, Lda
Country	C	C = PT

3.1.2 Need for names to be meaningful

The GTS ROOT 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 certificate's ***Subject CN***, is equal to one of the FQDN ***Subject Alternative Names***, which has been validated using at least one of the procedures in section 3.2.2.4 of the *CA/B Forum Baseline Requirements*.

3.1.3 Anonymity or pseudonymity of subscribers

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

3.1.4 Rules for interpreting various name 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 ROOT 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 ROOT 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 GTS trust hierarchy, it is mandatory that the GTS ROOT 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 the GTS ROOT CA self-signed certificate, proof of ownership of the private key will be guaranteed through the physical presence of the various relevant working groups at the ceremony for issuing this type of certificate. At this ceremony, the certificate request will be generated and presented in PKCS#10 format, whose signature on the public key information will be validated.

In cases in which the GTS ROOT 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 Organisation and Domain Identity

CNs issued by the GTS ROOT 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.

DP02 identifies more points regarding the authentication of the organisation.

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 Authorisation 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 Validation

Global Trusted Sign does not issue Wildcard certificates.

3.2.2.7 Data Source Accuracy

Global Trusted Sign 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.

Document DP02 shows how identity authentication is carried out according to the type of person.

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 recognised 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 recognised 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 recognised 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
- Organisation / 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 recognised 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 recognised 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 recognised 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 recognised 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 the information provided by the subscriber is verified.

3.2.5 Validation of authority

See Organisation 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

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

Other certificate subscription requests may be submitted by the following:

- The certificate holder;
- A representative of the certificate holder, duly authorised 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

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

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

- 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. A certificate request does not imply its obtainment in case the applicant does not meet the requirements established in this document. 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*.

Documents must be submitted in Portuguese or in a foreign language widely used at international level, such as English.

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

In the terms and conditions specific to each service, Global Trusted Sign refers to the time for issuing the certificates -FO31 – General Terms and Conditions.

4.3 Certificate issuance

The certificate issuance process is carried out by the GTS ROOT CA Registration Administrators through a specific procedure 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 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

Once the documentation has been received, a process is started to validate the information and identity of the holder and, where applicable, the requesting organisation. The process of issuing certificates is always carried out by two Registry Administrators, in order to guarantee double authentication. Only in this way is the authenticity of the data provided validated and confirmed.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The certificate is issued in person, according to the next section: Certificate acceptance.

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

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

4.4.2 Publication of the certificate by the CA

The GTS ROOT CA does not publish the list of issued certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

The GTS ROOT 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 the GTS ROOT CA.
- The GTS ROOT CA is the holder of the Global Trusted Sign Root Certification Authority 01 self-signed certificate. This certificate is used to sign the subordinate certification bodies that belong to the GTS ROOT CA hierarchy, as well as the Certificate Revocation List itself, under the terms defined in Certification Practice Statement (DP01).
- The ROOT key pair is not used to issue EV/OV certificates.

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 ROOT CA supplies in this Practice Statement and Certification Policy 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 ROOT 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 requests

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

Not stipulated.

4.7.2 Who may request certification of a new public key

Not stipulated.

4.7.3 Processing certificate re-keying 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 ROOT CA.

4.8.1 Circumstance for certificate modification

Not stipulated.

4.8.2 Who may request 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 ROOT 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.

Translated with DeepL.com (free version)

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

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

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

- When the GTS CA is aware of a demonstrated or proven method that can easily calculate the Private Key of the Subscriber based on the Public Key in the Certificate (as a Debian weak key, according to https://wiki.debian.org/SSLkeys);
- When the GTS CA 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 authorised;
- Use of the certificate for abusive activities.

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

- The certificate no longer meets the requirements set out in section 6.1.5 and section 6.1.6;
- The GTS ROOT CA has evidence that the certificate has been misused;
- The GTS ROOT CA is informed that the subscriber has violated one or more of his/her material obligations under the Terms and Conditions of Use;
- The GTS ROOT 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;
- The GTS ROOT CA is informed that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully qualified domain name;
- The GTS ROOT CA becomes aware of a material change in the information contained in the Certificate;
- The GTS ROOT CA is aware that the certificate was not issued in conformity with these Requirements or with the Certificate Policy or Certification Practices Statement of the CA;
- The GTS ROOT CA determines or is informed that any of the information contained in the Certificate is inaccurate;

- The right of the GTS ROOT 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;
- Revocation is required in accordance with the Certification Policy and/or Certification Practices Statement of the GTS ROOT CA; or
- The GTS 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.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

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

4.9.2 Who can request revocation

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

- The Certificate holder;
- The Certification Authority or Requesting Entity of the certificate of the subordinate entity;
- Global Trusted Sign, 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

The revocation requests of the self-signed certificate of the GTS ROOT CA, shall be addressed in writing or by electronic message digitally signed by the Management of Acin iCloud Solutions, Lda. The entity is then identified, and the respective request is registered and filed. After analysis by the Global Trusted Sign 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 exhibition of the motives 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 submits the revocation request.

For other certificates, the 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.

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

4.9.5 Time within which CA must process the revocation request

After the revocation request is made and the signed documentation is sent, it shall not exceed 24 hours.

After confirmation of the applicant's identity and authenticity, the TSP shall proceed, within 60 minutes, to change the certificate status to revoked, upon receipt and validation of the required documentation.

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 ROOT CA can be checked by consulting the CRL, which is issued whenever certificates are revoked or, in the absence of any change in certificate status, on a quarterly basis. The CRL is made available in the repositories within no more than 30 minutes and can be downloaded in less than 10 seconds. To ensure its availability, the CRL is published in the following repositories:

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

4.9.8 Maximum latency for CRLs (if applicable)

Global Trusted Sign has sufficient resources to ensure normal operating conditions, namely a response time for CRL and OCSP services of less than or equal to 10 seconds.

4.9.9 On-line revocation/status checking availability

The Global Trusted Sign ROOT CA provides an OCSP service for online certificate status validation. This service is accessible at http://ocsp.globaltrustedsign.com.

4.9.10 On-line 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 or https://pki02.globaltrustedsign.com/index.html, ensuring its availability 24 hours a day, 7 days a week, except during scheduled maintenance periods duly communicated to the relevant parties.

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 Practice Statement and Certification Policy, the parties may use the email report@globaltrustedsign.com to demonstrate the compromising of the private key of the subscribed certificates.

4.9.13 Circumstances for suspension

The certificate suspension process is not supported by Global Trusted Sign.

4.9.14 Who can request suspension

Not stipulated.

4.9.15 Procedure for suspension request

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 ROOT 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 ROOT CA shall have at least one backup copy, maintained with the same level of security as the original key, and shall be subject to secure backup procedures;
- They are stored in encrypted form in HSM.

4.12.2 Session key encapsulation and recovery policy and practices

See section 4.12.1.

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

5.1 Physical Security Controls

5.1.1 Site location and construction

The GTS ROOT 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:

- Handling subscriber information and validating certificate issue information;
- Functions of the certificate life cycle;
- Configuration and maintenance of certification systems.

Within the scope of its organisational 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 authorised 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 Global Trusted Sign Policies and Practice Statements
- Safeguard of artefacts under its custody.

5.2.2 Number of Individuals Required per Task

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

5.2.3 Identification and authentication for each role

See section 5.2.1.

5.2.4 Roles requiring separation of duties

The composition of the working groups must respect the principles of minimum privilege and segregation of functions. The following table shows the incompatibilities between the different groups existing in 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;
- Global Trusted Sign 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 unauthorised 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 unauthorised access, amendments, manipulation or destruction attempts. As a rule, electronic records must be protected using cryptographic techniques so nobody, except the own records visualisation 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 ROOT 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 collection System (internal vs. external)

Logs are centrally collected and processed.

5.4.7 Notification to event-causing subject

Auditable events are recorded in Global Trusted Sign's internal systems and are stored securely. No notification to the agent responsible for the event is provided.

5.4.8 Vulnerability assessments

Although no significant changes occur in the ROOT 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 and Certification Policy, 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 ROOT CA shall archive at least 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 ROOT CA shall ensure the recording of the date and time of each event, based on a secure time source.

5.5.6 Archive collection system (internal or external)

See section 5.4.6.

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key changeover

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 the event of a major security incident or compromise of the ROOT 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 ROOT CA or its subscribers become insufficient for their intended purpose, the ROOT CA shall:

- Inform all holders and other entities with which the ROOT 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 PKI hierarchy;
- Schedule the revocation of any affected certificate.

5.7.4 Business continuity capabilities after a disaster

Global Trusted Sign maintains a business continuity plan describing all procedures to be activated in the event of a disaster resulting in loss or corruption of data, software, or equipment. The Business Continuity Plan shall ensure that services identified as critical in terms of availability are provided from an alternate site, and that ROOT CA data required to resume operations is backed up and stored in secure and appropriate locations to enable the proper restoration of ROOT CA operations in the event of incidents or disasters. Backups of essential information and software are performed regularly. Appropriate supporting facilities shall be provided to ensure that all essential information and software can be recovered after a disaster or failure of communication media. Safeguard mechanisms shall be tested regularly to ensure that they meet the requirements of the business continuity plans.

5.8 CA or RA termination

In the event of termination of operations, Global Trusted Sign shall, in a timely manner, carry out 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 the ROOT CA;
- Revocation of all certificates;
- Ensure the transfer (for its retention by another organisation) 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 organisation) of all information regarding the ROOT 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 ROOT CA activity, the GTS ROOT 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 PKI in order to protect the cryptographic keys generated by it and their respective activation data. The security level assigned to key management shall be the highest, ensuring that private keys and secure keys, as well as activation data, are always protected and accessible only to duly authorised persons. The generation of the ROOT CA key pairs is carried out in accordance with the requirements and algorithms defined in this document.

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

The generation of key pairs of the 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 Subscriber Key Pair Generation

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*. The size defined for the keys is the following:

- 4096 bits RSA for the key of the GTS certification 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 mandatory performed directly within a hardware cryptographic module (HSM). The cryptographic module complies with FIPS 140-2 Level 3 requirements. These certificates are signed by the ROOT CA. The ROOT CA operates in offline mode.

The ROOT CA key pair generation shall be performed in accordance with PKCS#11 specifications.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The ROOT CA certificate key pair is intended to:

- Sign the CAs certificates;
- Sign the Offline CRL;
- Sign the CRL.

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 ROOT CA uses cryptographic modules (HSMs) for operations related to key generation, storage, and signing. The cryptographic modules comply with Common Criteria v2.3, FIPS 140-2, and FIPS 140-2 Level 3 (for the ROOT CA cryptographic module). The security of the ROOT CA cryptographic module is ensured throughout its lifecycle, ensuring the following:

- The installation and activation of keys in the cryptographic module is conducted by members of the working groups duly identified (section 5.2, Procedural Controls, and section 5.3, Personnel Controls);
- 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 ROOT 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 ROOT 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 ROOT 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

See section 6.2.3.

6.2.5 Private key archival

See section 6.2.3.

6.2.6 Private key transfer into or from a cryptographic module

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

6.2.7 Private key storage on cryptographic module

See section 6.2.3.

6.2.8 Activating Private Keys

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

6.2.9 Deactivating Private Keys

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

6.2.10 Destroying Private Keys

The ROOT 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 Rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The ROOT 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 ROOT CA certificate has a minimum validity of 20 years;
- A certificate for a subordinate entity issued by the ROOT CA has a minimum validity of 1 year, and a maximum of 6 or 8 years.

6.4 Activation data

6.4.1 Activation data generation and installation

See section 6.2.2.

6.4.2 Activation data protection

The private key activation data is stored in safe environments (see section 6.2: Private key protection and cryptographic module engineering controls).

6.4.3 Other aspects of activation data

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

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Access to the 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 authorised members of the ROOT CA. The ROOT CA has mechanisms to control and monitor the ROOT 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 ROOT 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 CA is recorded with the date and time of creation. The entire infrastructure is time-synchronised using an internal atomic clock, and additionally through 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 ROOT 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 ROOT CA GTS certificate profiles can be found at: https://pki.globaltrustedsign.com/index.html and https://pki02.globaltrustedsign.com/index.html,or below.

a) Profile of the GTS ROOT CA Self-Signed Certificate

OID	Certificate Component	Value	Type	Remarks
	Version	V3	M	
	Serial Number	<Assigned by the CA to each certificate>	M	Unique identifier of the certificate
1.2.840.113549.1.1.11	**Signature**	sha256WithRSAEncryption	M	Certificate signature
	Issuer		M	
	Country (C)	"PT"		
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	Global Trusted Sign Root Certification Authority 01		
	Validity		M	Validity of the Certificate

OID	Certificate Component	Value	Type	Remarks
	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"		
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	<Fully Qualified Domain Name of the Certification Authority>		
	Subject Public Key Info		M	
1.2.840.113549.1.1.1	Algorithm	rsaEncryption		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 Certification Authorities
	PathLenConstraint	None		
1.2.840.113549.1.1.11	**Signature Algorithm**	sha256WithRSAEncryption	M	Algorithm used to create the certificate signature.
	Signature Value	<It contains the digital signature issued by the ROOT CA>	M	Certificate signature

b) Profile of Certificate for Qualified Certification Authority 01 - SUBCAO1

OID	Certificate Component	Value	Type	Remarks
	Version	V3	M	
	Serial Number	<Assigned by the CA to each certificate>	M	Unique identifier of the certificate
1.2.840.113549.1.1.11	**Signature**	sha256WithRSAEncryption	M	Certificate signature

OID	Certificate Component	Value	Type	Remarks
	Signature hash algorithm	Sha256		
	Issuer		M	
	Country (C)	"PT"		
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation 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>		11/08/2017
	Valid to	<Date of issuance + 20 years>		Maximum validity of 6 years
	Subject		M	
	Country (C)	"PT"		
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	"Global Trusted Sign Certification Authority 01"		<CA Fully Qualified Domain Name >
	Subject Public Key Info		M	
1.2.840.113549.1.1.1	Algorithm	rsaEncryption		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	Identifier of the certificate key
	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 Signature	"1" selected		
	Encipher Only	"0" selected		
	Decipher Only	"0" selected		
	Certificate Policies		M	
1.3.6.1.4.1.50302.1.1.1.2.1.0	policyIdentifier			Identifier and location of the GTS CA Certification Practices Statement

OID	Certificate Component	Value	Type	Remarks
	policyQualifiers	Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Location of the GTS CA Certification Practices Statement
	Basic Constraints		M	
	Subject Type	CA		Certificate intended for Certification Authorities
	PathLenConstraint	None		
	CRLDistributionPoints		M	
	[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_root_crl.crl		Location of the GTS ROOT CA Certificate Revocation List
	[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_root_crl.crl		Secondary location of the GTS ROOT CA Certificate Revocation List
	Authority Information Access		M	
1.3.6.1.5.5.7.48.2	accessMethod	Certification Authority Issuer		Parameter used to identify the GTS ROOT CA certificate and build the chain of trust.
	accessLocation	https://pki.globaltrustedsign.com/root/gts_root.crt		Location of the GTS ROOT CA Certificate
1.2.840.113549.1.1.11	**Signature Algorithm**	sha256WithRSAEncryption	M	Algorithm used for creating the Certificate signature.
	Signature Value	<It contains the digital signature issued by the GTS CA>	M	Certificate signature

c) Profile of Certificate for Qualified Certification Authority 03 – SUBCA03

OID	Certificate Component	Value	Type	Remarks
	Version	V3	M	
	Serial Number	<Assigned by the CA to each certificate>	M	Unique identifier of the certificate
1.2.840.113549.1.1.11	**Signature**	sha256WithRSAEncryption	M	Certificate signature
	Signature hash algorithm	sha256		
	Issuer		M	
	Country (C)	"PT"		
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	"Global Trusted Sign Root Certification Authority 01"		
	Validity		M	Certificate Validity
	Valid from	<Date of issuance>		11/05/2020
	Valid to	< Date of issuance + 8 years>		Maximum validity of 8 years
	Subject		M	

OID	Certificate Component	Value	Type	Remarks
	Country (C)	"PT"		
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	"Global Trusted Sign Certification Authority 03"		< CA Fully Qualified Domain >
	Subject Public Key Info		M	
1.2.840.113549.1.1.1	Algorithm	rsaEncryption		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	Identifier of the certificate key
	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 Signature	"1" selected		
	Encipher Only	"0" selected		
	Decipher Only	"0" selected		
	Certificate Policies		M	
1.3.6.1.4.1.50302.1.1.1.2.1.0	policyIdentifier			Identifier and location of the GTS CA Certification Practices Statement
	policyQualifiers	Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Location of the GTS CA Certification Practices Statement
	Basic Constraints		M	
	Subject Type	CA		Certificate intended for Certification Authorities
	PathLenConstraint	None		
	CRLDistributionPoints		M	
	[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_root_crl.crl		Location of the GTS ROOT CA Certificate Revocation List
	[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_root_crl.crl		Secondary location of the GTS ROOT CA Certificate Revocation List
	Authority Information Access		M	

OID	Certificate Component	Value	Type	Remarks
1.3.6.1.5.5.7.48.2	accessMethod	Certification Authority Issuer ()		Parameter used to identify the GTS ROOT CA certificate and build the chain of trust.
	accessLocation	https://pki.globaltrustedsign.com/root/gts_root.crt		Location of the GTS ROOT CA Certificate
1.2.840.113549.1.1.11	**Signature Algorithm**	sha256WithRSAEncryption	M	Algorithm used for creating the Certificate signature.
	Signature Value	<It contains the digital signature issued by the GTS CA>	M	Certificate signature

d) Profile of Certificate for Subordinate Non-Qualified Certification Authority 02 – SUBCANQ02

OID	Certificate Component	Value	Type	Remarks
	Version	V3	M	
	Serial Number	<Assigned by the Certification Authority to each certificate>	M	Unique identifier of the certificate.
1.2.840.113549.1.1.11	**Signature**	sha256WithRSAEncryption	M	Certificate signature.
	Signature algorithm	sha256		
	Issuer		M	
	Country (C)	"PT"		
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	Global Trusted Sign Root Certification Authority 01		
	Validity		M	Certificate Validity
	Valid from	<Date of issuance>		23/03/2019
	Valid to	<Date of issuance + 6 years>		Maximum validity of 6 years.
	Subject			
	Country (C)	<PT>	M	Country of the nationality of the certificate holder
	Organisation (O)	"ACIN iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	"Global Trusted Sign NQ Certification Authority 02"		<Non-Qualified CA Fully Qualified Domain Name >
	Subject Public Key Info		M	
1.2.840.113549.1.1.1	Algorithm	rsaEncryption		Public Key algorithm
	subjectPublicKey	<Public Key>		Certificate Public Key
	Authority Key Identifier		M	
	keyIdentifier	160-bit hash		It allows to identify the public key corresponding to the private key of the certificate
	Subject Key Identifier	160-bit hash	M	Identifier of the certificate key
	Key Usage		M	
	Digital Signature	"0" selected		
	Non-Repudiation	"0" selected		

OID	Certificate Component	Value	Type	Remarks
	Key Encipherment	"0" selected		
	Data Encipherment	"0" selected		
	Key Agreement	"0" selected		
	Key Certificate Signature	"1" selected		
	CRL Signature	"1" selected		
	Off-line CRL Signature	"1" selected		
	Encipher Only	"0" selected		
	Decipher Only	"0" selected		
	Certificate Policies		M	
1.3.6.1.4.1.50302.1.1.1.1.1.0	policyIdentifier	**policyIdentifier:**		Identifier and location of the GTS CA Certification Practices Statement
	policyQualifiers	Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identifier and location of the GTS CA Certification Practices Statement
	Basic Constraints		M	
	Subject Type	CA		Certificate intended for Certification Authorities
	PathLenConstraint	None		
	CRLDistributionPoints		M	
	[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_root_crl.crl		Location of the GTS ROOT CA Certificate Revocation List
	[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_root_crl.crl		Secondary location of the GTS ROOT CA Certificate Revocation List
	Authority Information Access		M	
1.3.6.1.5.5.7.48.2	accessMethod	Certification Authority Issuer		Parameter used to identify the GTS ROOT CA certificate and build the chain of trust.
	accessLocation	https://pki.globaltrustedsign.com/root/gts_root.crl		Location of the GTS ROOT CA certificate
1.2.840.113549.1.1.11	**Signature Algorithm**	sha256WithRSAEncryption	M	Algorithm used for creating the Certificate signature
	Signature Value	<It contains the digital signature issued by the NQCA>	M	Certificate signature

e) Profile of Certificate for Subordinate Non-Qualified Certification Authority 03 – SUBNQ03

OID	Certificate Component	Value	Type	Remarks
	Version	V3	M	
	Serial Number	<Assigned by the Certification Authority to each certificate>	M	Unique identifier of the certificate.
1.2.840.113549.1.1.11	**Signature**	sha256WithRSAEncryption	M	Certificate signature.
	Issuer		M	
	Country (C)	"PT"		

OID	Certificate Component	Value	Type	Remarks
	Organisation (O)	"ACIN-iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	Global Trusted Sign Root Certification Authority 01		
	Validity		M	Certificate Validity
	Valid from	<Date of issuance>		14/07/2022
	Valid to	< Date of issuance + 8 years>		Maximum validity of 8 years.
	Subject			
	Country (C)	<País>	M	Country of the nationality of the certificate holder
	Organisation (O)	"ACIN iCloud Solutions, Lda"		
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	"Global Trusted Sign NQ Certification Authority 03"		<Non-Qualified CA Fully Qualified Domain Name >
	Subject Public Key Info		M	
1.2.840.113549.1.1.1	Algorithm	rsaEncryption		Public Key algorithm
	subjectPublicKey	<Public Key>		Certificate Public Key
	Authority Key Identifier		M	
	keyIdentifier	160-bit hash		It allows to identify the public key corresponding to the private key of the certificate
	Subject Key Identifier	160-bit hash	M	Identifier of the certificate key
	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 Signature	"1" selected		
	Encipher Only	"0" selected		
	Decipher Only	"0" selected		
	Certificate Policies		M	
1.3.6.1.4.1.50302.1.1.1.1.1.0	policyIdentifier	policyIdentifier		Identifier and location of the GTS CA Certification Practices Statement
	policyQualifiers	Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identifier and location of the GTS CA Certification Practices Statement
	Basic Constraints		M	

OID	Certificate Component	Value	Type	Remarks
	Subject Type	CA		Certificate intended for Certification Authorities
	PathLenConstraint	None		
	CRLDistributionPoints		M	
	[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_root_crl.crl		Location of the GTS ROOT CA Certificate Revocation List
	[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_root_crl.crl		Secondary location of the GTS ROOT CA Certificate Revocation List
	Authority Information Access		M	
1.3.6.1.5.5.7.48.2	accessMethod	Certification Authority Issuer		Parameter used to identify the GTS ROOT CA certificate and build the chain of trust.
	accessLocation	https://pki.globaltrustedsign.com/root/gts_root.crl		Location of the GTS ROOT CA certificate
1.2.840.113549.1.1.11	**Signature Algorithm**	sha256WithRSAEncryption	M	Algorithm used for creating the Certificate signature
	Signature Value	<It contains the digital signature issued by the NQCA>	M	Certificate signature

f) Profile of the Certificate of the Timestamping Authority 002 – TSA002

OID	Certificate Component	Value	Type	Remarks
	Version	V3	M	
	Serial Number	<Assigned by the CA to each certificate>	M	
1.2.840.113549.1.1.11	**Signature**	sha256WithRSAEncryption	M	Certificate signature. Value must be equal to the OID in the *SignatureAlgorithm* (below)
	Issuer		M	
	Country (C)	"PT"		Country of the issuing authority
	Organisation (O)	"ACIN iCloud Solutions, Lda"		Name of the organisation of the issuing authority
	Organisation Unit (OU)	"Global Trusted Sign"		
	Common Name (CN)	Global Trusted Sign Certification Authority 01		
	Validity			Certificate Validity
	Valid from	<Date of issuance>		14/07/2022

OID	Certificate Component	Value	Type	Remarks
	Valid to	< Date of issuance + 8 years>		Maximum validity of 8 years
	Subject		M	
	Country (C)	PT		Country of the nationality of the certificate holder
	Organisation (O)	ACIN iCloud Solutions, Lda		
	Organisation Unit (OU)	Global Trusted Sign		
	Common Name (CN)	Global Trusted Sign Timestamping Authority 002		
	Subject Public Key Info		M	
1.2.840.113549.1.1.1	Algorithm	rsaEncryption		Public Key algorithm
	subjectPublicKey	<Public Key>		Certificate Public Key
	Authority Key Identifier		M	
	keyIdentifier	160-bit hash		It allows to identify the public key corresponding to the private key of the certificate
	Subject Key Identifier	160-bit hash	M	Identifier of the certificate key
	Key Usage		M	
	Digital Signature	"1" selected		
	Non-Repudiation	"1" selected		
	Key Encipherment	"0" selected		
	Data Encipherment	"0" selected		
	Key Agreement	"0" selected		
	Key Certificate Signature	"0" selected		
	CRL Signature	"0" selected		
	Encipher Only	"0" selected		
	Decipher Only	"0" selected		
1.3.6.1.5.5.7.3.8	**Enhanced Key Usage**	Time Stamping		
	Certificate Policies		M	

OID	Certificate Component	Value	Type	Remarks
1.3.6.1.4.1.50302.1.1.1.3.1.0	[1]	policyIdentifier: Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identifier and location of the GTS TSA Certification Practices Statement
1.3.6.1.4.1.50302.1.1.2.3.1.0	[2]	BST policy-identifier: 0.4.0.2023.1.1 Own policyIdentifier: 1.3.6.1.4.1.50302.1.1.2.3.1.0 cPSuri: https://pki.globaltrustedsign.com/index.html		best-practices-ts-policy Identifier and location in the Timestamp Certificate policy
	Basic Constraints		M	
	Subject Type	End Entity	C	Certificate intended for Timestamping
	PathLenConstraint	None		
	CRLDistributionPoints		M	
	[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_subca_crl.crl		Location of the GTS SUBCA Certificate Revocation List
	[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_subca_crl.crl		Secondary location of the GTS SUBCA Certificate Revocation List
1.2.840.113549.1.1.11	**Signature Algorithm**	sha256WithRSAEncryption	M	Algorithm used for creating the Certificate signature
	Signature Value	<It contains the digital signature issued by the CA>	M	Certificate signature

M – Mandatory, O – Optional

* - (*Given Name* (G) and *Surname* (SN)) or (*Organisation* (O) with Pseudonym) is Mandatory.

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 on certificate profiles can be consulted in section 7.1 of this document and via access to the repository at https://pki.globaltrustedsign.com/ and https://pki02.globaltrustedsign.com/index.html, as well as in the previous section.

7.1.2.2 Subordinate CA certificate

See section 7.1.2.1.

7.1.2.3 Certificate subscribers

The information is available in the archived certificates, accessible via the repository at https://pki.globaltrustedsign.com/index.html and https://pki02.globaltrustedsign.com/index.html.

7.1.2.4 All certificates

The information is available in the archived certificates, accessible via the repository at https://pki.globaltrustedsign.com/index.html and https://pki02.globaltrustedsign.com/index.html repository and through PL01_GTS - Qualified Certificate Policy; PL16_GTS – Non-Qualified Certificate Policy and PL14_GTS – Timestamp Certificate Policy.

7.1.2.5 Applicability 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 requirements of the Public Key parameter field available in the certificates apply.

7.1.3.1 SubjectPublicKeyInfo

Information available in the certificate profiles set out in section 7.1 of this document and at https://pki.globaltrustedsign.com/index.html and https://pki02.globaltrustedsign.com/index.html.

7.1.3.2 Signature AlgorithmIdentifier

The ***signatureAlgorithm*** field of the certificate contains the OID of the cryptographic algorithm used by the TSA 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 extension "*certificate policies*" is not active in the self-signed certificate of the ROOT CA.

All certificates issued by the 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.

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 extension

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 ROOT 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 PKI comply with version 1 of RFC 6960.

7.3.2 OCSP extensions

Not stipulated.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Global Trusted Sign shall perform regular audits and compliance assessments to ensure that the Certification Authorities within its trust hierarchy comply with national legislation as well as applicable international standards.

8.1 Frequency or circumstances of assessment

At the ROOT 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.

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 ROOT CA holders' files.

8.4 Topics covered by assessment

A security audit is conducted on the basis of the requirements defined in this document and in compliance with applicable national legislation. It aims to determine the conformity of the ROOT CA services defined in the Practices Statement and Certificate Policies. 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–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 Global Trusted Sign Trust Group, according to the guidelines adopted by the CA/B Forum.

Significant events that generate auditable records are considered to be the following:

– Security related events, including:
  - Attempts to access (successful and unsuccessful) sensitive resources of ROOT CA
  - Operations carried out by members of the Working Groups
  - Physical input/output security devices of several levels of safety.

– Requests for the issuance of certificates

– CRL updates;

Record entries include the following information:

– Event category;

– Date and Time of the event;

– Event description;
– Identity of the incident causative agent;
– Serial number of the event.

Audit records are kept available for at least 1 month after processing, and are subsequently 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

Global Trusted Sign maintains a civil liability insurance contract intended to ensure adequate coverage of civil liability arising from the provision of trust services, in accordance with Decree-Law No. 12/2021 of 9 February and Ministerial Order No. 62/2021 of 17 March, as well as Regulation (EU) No. 910/2014 (eIDAS), in its consolidated version as amended by Regulation (EU) 2024/1183.

9.2.2 Other assets

Not stipulated.

9.2.3 Insurance or warranty coverage for end-entities

Global Trusted Sign maintains a civil liability insurance contract intended to cover risks arising from the provision of qualified trust services, in accordance with Regulation (EU) No 910/2014 (eIDAS), in its consolidated version as amended by Regulation (EU) 2024/1183, as well as Decree-Law No. 12/2021 of 9 February and Ministerial Order No. 62/2021 of 17 March.

The civil liability insurance ensures coverage for damages that may result from non-compliance with the legal and regulatory obligations arising from the activity of a Qualified Trust Service Provider, under applicable legislation.

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 the ROOT CA during the registration process of certificate subscribers, unless there is an explicit authorisation for its disclosure;
- Business continuity and recovery plans;
- Transactions records, including complete records and audit records of transactions;
- Data on members of the ROOT CA working groups.

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

9.3.3 Responsibility to protect confidential information

The ROOT CA practices ensure the protection of the confidentiality and integrity of registration data, particularly when transmitted between the ROOT CA and subscribers and certificate holders, as well as during communication between distributed components of the ROOT CA systems. Within the scope of the services provided, it is necessary to maintain digital evidence for compliance purposes with applicable legislation governing the ROOT CA. This evidence is maintained in a way that ensures its secure 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 to 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 ROOT 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 ROOT CA is obliged to comply with the following directives:

- To conduct its operations in accordance with this Practice Statement and Certification Policy;
- 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 recognised 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 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 the ROOT 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 ROOT 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 ROOT CA certificates.

9.6.2 RA representations and warranties

The Registration Authority (RA) is the entity responsible for analysing and evaluating the requests for Global Trusted Sign 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

Nothing to report as this is the ROOT Certification Practice Statement and Certification Policy.

9.6.4 Relying party representations and warranties

Nothing to report as this is the ROOT Certification Practice Statement and Certification Policy.

9.6.5 Representations and warranties of other participants

Not stipulated.

9.7 Disclaimers of warranties

The GTS CA disclaims all service warranties that are not bound to the obligations established in this ROOT Certification Practice Statement and Certification Policy.

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 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 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 Global Trusted Sign 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 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 ROOT Certification Practice Statement and Certification Policy shall enter into force upon its publication in the ROOT CA repository and after its approval, under the terms of this document. This document shall remain in force until it is expressly revoked by the issuance of a new version, in accordance with this document, or by the renewal of the ROOT CA keys, at which point a new version shall mandatorily be drafted.

9.10.2 Termination

This ROOT Certification Practice Statement and Certification Policy 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 ROOT Certification Practice Statement and Certification Policy 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 TROOT Certification Practice Statement and Certification Policy, related to audits, confidential information, obligations and responsibilities of the 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 Practice Statement and Certification Policy must be approved by the Management Group. Amendments must be carried out through documents, containing the new amendments to the Practice Statement and Certification Policy.

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 CA determines that a change to the identifier (OID) of the Practice Statement and Certification 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 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 governmental authority with jurisdiction over the activities covered by this Certification Practice Statement and Certificate Policy determines that compliance with any mandatory requirement is illegal or not appropriate in the country where the CA is implemented, such requirement shall be deemed reformed to the minimum extent necessary to make it valid and lawful. This shall apply only to operations or certificate issuances subject to the laws of that jurisdiction. Global Trusted Sign undertakes to notify the CA/Browser Forum of 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 Practice Statement and Certification Policy, including limitation of liability clauses, is found to be ineffective or unenforceable, the remainder of this Practice Statement and Certification Policy shall be construed in the sense of the original intention of the parties. Any provision of this Practice Statement and Certification Policy 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 (attorneys' fees and waiver of rights)

Not stipulated.

9.16.5 Force Majeure

Not stipulated.

9.17 Other provisions

Not stipulated.