GTS CA DISCLOSURE OF PRINCIPLES STATEMENT

Global Trusted Sign

Document Reference | DP04_GTS_V7

TABLE OF CONTENTS

1. References	European Regulation Nº 910/2014 ETSI 319 411-1 ETSI 319 412 ETSI 319 401 RFC 5280: Internet X.509 PKI - Certificate and CRL Profile, 2008 CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.7; ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, v2.4.1
2. Related Documents	DP01_GTS – Root GTS CA Certification Practice Statement
3. Distribution List	Interested parties in the GTS CA trust hierarchy
4. Document History	31-07-2017 | Version 1 29-12-2017 | Version 2 16-04-2018 | Version 3 05-04-2019 | Version 4 04-05-2020 | Version 5 24-06-2020 | Version 6 17-09-2020 | Version 7
5. Document Classification	D | Public

6. Revision

Version Number	Creation	Approval	Reason
	17-09-2020	17-09-2020	
7	**AdmSeg**	**Management Group**	Update of GTS Trust Group and registrations.
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 17-09-2020 17:54:20	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 17-09-2020 17:56:18	

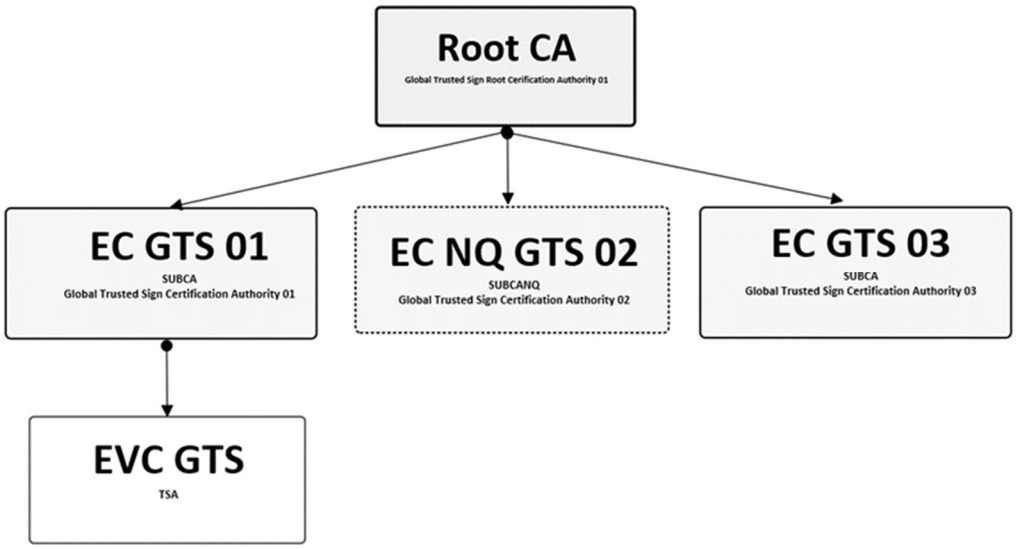
7. Introduction

7.1. Purpose

This document is intended to summarize, in a simple and accessible manner, the features described in the Certification Practice Statement and Certification Policy of the Global Trusted Sign Certification Authority (hereinafter referred to as GTS Certificate Authority or GTS CA).

The infrastructure of the GTS CA provides a trust hierarchy that promotes an electronic security of the digital certificate subject. The GTS CA establishes an electronic trust structure that provides secure electronic transactions, strong authentication, a mean for electronically signing transactions or electronic documents, ensuring its accountability, integrity and non-repudiation, and guaranteeing the confidentiality of transactions or information.

The GTS CA is a certification authority accredited by the National Security Office (*Gabinete Nacional de Segurança*) (http://www.gns.gov.pt/trusted-lists.aspx), as defined in the Portuguese and European legislation, and is thus legally entitled to issue several types of qualified digital certificates. GTS CA is signed by the ROOT GTS CA, thus belonging to the trust hierarchy, represented in the following figure:



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

7.2. Target Audience

This document should be read by the holders and subscribers of certificates issued by the GTS CA.

7.3. Document Structure

This document is organized in accordance with ETSI EN 319 411-1.

This document is the GTS CA Disclosure of Principles Statement, and its associated OID is 1.3.6.1.4.1.50302.1.1.3.2.1.0, while the OIDs associated with the GTS CA Certificate Policies are 1.3.6.1.4.1.50302.1.1.2.2.1.0 and 1.3.6.1.4.1.50302.1.1.2.4.1.0:

Document information	
Document Name	GTS CA Disclosure of Principles Statement
Document Version	7.0
Document Status	Approved
OID	1.3.6.1.4.1.50302.1.1.3.2.1.0
Issuance Date	17th September 2020
Validity	17th September 2021
Location	https://pki.globaltrustedsign.com/index.html

Note: Updates to this document are conducted when changes in legal or local procedures are produced, or where applicable.

8. Contacts of the GTS Certification Authority

Name	GTS Certification Authority Management Group
Address	ACIN iCloud Solutions Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira Portugal
E-mail	info@globaltrustedsign.com
Phone	707 451 451

Suspension/Revocation request must be submitted through the portal available at: https://www.globaltrustedsign.com.

9. Types of certificates, validation and use procedures

9.1. Certificate Use

Qualified certificates for website authentication issued by the GTS CA are used by different holders, systems, mechanisms, and protocols, with the aim to establish the transmission of web-based data through SSL/TLS protocols.

This ensures efficient and secure electronic communications, while the concern of users regarding the trust of the certificates is addressed.

9.1.1. Proper Use

Requirements and provisions set forth in this Disclosure of Principles Statement are applicable to all certificates issued by the GTS CA. These certificates aim to:

- Identify the legal entity that controls a website: it provides reasonable assurance to the user of an Internet browser that the site to which the user will access is controlled by a legal entity identified in the certificate by its name, registered office, registration in the *Instituto de Registos e Notariado* (Institute of Registries and Notaries), or any other disambiguating information.

- Allow encrypted communications with a website: it facilitates the exchange of encryption keys to allow transmission of encrypted information through Internet, between an Internet browser user and a website.

By providing a process for verification of identity more reliable and information of the registered office of the company, the *Extended Validation* (EV) certificates can help to:

- Prevent phishing attacks and other frauds of the identity used in the certificates;

- Support companies that have been targeted in phishing or identity fraud by making available to users a tool for its identification;

- Support the security forces in their investigations of phishing and other attacks of identity fraud, contributing, where applicable, contact, investigation, and legal actions against the holder.

Relying Parties may verify the chain of trust of a certificate issued by the GTS CA, thus ensuring the authenticity and identity of the subject.

9.1.2. Unauthorised Certificate Uses

Qualified certificates for website authentication issued by the GTS CA are focused on the identity of the Certificate holder, and not on his/her behaviour. Therefore, a website authentication certificate gives no guarantee that:

- The holder identified in the certificate is in fact providing the service;

- The holder identified in the certificate is acting in accordance with the applicable legislation;

- The holder identified in the certificate is reliable, honest or ethical in the execution of his/her activities;

- Is "safe" to establish a business relationship with the holder identified in the certificate.

9.2. Validation Procedures

Qualified certificates for website authentication issued by the GTS CA are trusted in the public context and comply with the following documents:

- GTS CA Certification Practices Statement:
    - Defines the practices followed by GTS CA for certificate lifecycle management (OID: 1.3.6.1.4.1.50302.1.1.1.2.1.0)
- GTS CA Certificate Policies:
    - SSL EV: defines the profile of Web Site Authentication Certificates with Extended Validation (OID: 1.3.6.1.4.1.50302.1.1.2.2.1.0)
    - SSL OV: defines the profile of Web Site Authentication Certificates with Organization Validation (OID: 1.3.6.1.4.1.50302.1.1.2.4.1.0)

CRL can be accessed in https://pki.globaltrustedsign.com/index.html, assuring their availability 24 hours a day, 7 days a week, except in the event of a scheduled maintenance stop and properly communicated to the involved parties.

10. Limitation of trust in certificates

10.1. Certificate Usage

The use of the certificates issued to the subject must comply with the described in the respective certificate policies available at https://www.pki.globaltrustedsign.com/index.html.

Certificates issued by the GTS CA are also used by the Relying Parties to verify the trust chain of a certificate issued by subordinated certifying authorities of the GTS CA trust hierarchy, as well as to ensure the authenticity and identity of the issuer of a digital signature generated by the private key corresponding to the public key contained in a certificate.

Certificates may be used in other contexts only to the scope permitted by applicable law.

Certificates issued by the GTS CA shall not be used for any function outside the scope of the uses described above.

Qualified trust services provided by the GTS CA are not authorized for use in high risk activities or requiring a faultless activity, such as:

- Operation of hospital facilities;
- Operation of nuclear facilities;
- Air traffic control;
- Rail traffic control;
- Or any other activity where a failure could lead to death, personal injuries or serious damage to the environment.

10.2. Audit Records

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

– Security related events, including:

  - Attempts to access (with and without success) sensitive resources of the GTS 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;

The 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 then archived in accordance with national law.

11. Holder Responsibilities

Certificate holders shall use their private key only for the purposes of which they are intended (as established in the *keyUsage* certificate field) and always for legal purposes.

The use of certificates is only allowed:

- To whom is mentioned in the *Subject* field of the certificate and,
- As long as the certificate remains valid (active status) and is not in the CRL of the GTS CA.

The certificate holder must request the revocation of a certain certificate, whenever there is knowledge or suspicion of the compromise of its private key, or any other act that recommends this action. The GTS CA stores all documentation used to verify the identity and authenticity of the entity requesting revocation.

A certificate may be revoked if any of the following conditions are met:

- Compromise or suspected compromise of the private key or the private key password;
- Loss of the private key;
- Serious inaccuracies in the information provided;
- The compromise or suspected compromise of the GTS CA private key;
- Failure to comply with the responsibilities by the Certification Authority or certificate subject;

- Whenever there are credible reasons to suggest that the certification services may have been compromised in such a way that questions the reliability of the certificates;
- By judicial or administrative resolution.

When using the certificate and its public key, the subject must ensure that the following conditions are met:

- Be aware of and understand the use and functionality provided by public key cryptography;
- Be responsible for its correct use;
- Read and understand the terms and conditions described in the Certification Policies and Certification Practice Statements;
- Verify and validate the trust chains of the certificates;
- Verify the Certificate Revocation Lists (CRL) with special attention to their extensions marked as critical and purpose of the certificate (*keyUsage*) in question;
- Trust the certificates, using them whenever they are valid.

12. Verification of Certificate Status issued by GTS CA

Other parties who rely on the certificates issued by GTS CA must:

- Use the CRL query mechanisms listed above, and check the status of the certificate at the time of its use. It is your responsibility to verify it;
- Comply with to the specified in the Certificate Policies of the certificate in question (https://www.pki.globaltrustedsign.com/index.html);
- Use the certificate appropriately in accordance with the purposes of its issuance.

13. Limitations and Responsibilities

The GTS CA:

a) shall answer for damages and losses caused to any person in the exercise of its activity in accordance with Art.º 26 of DL 62/2003.

b) shall answer for losses caused to the subjects 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) shall take responsibility over the risks that individuals may suffer as a consequence of normal, or abnormal operation of its services.

d) only shall answer for damages and losses caused by improper use of recognized certificates, when the limitations to the possible use is not stated in the certificates, in a way that is clearly acknowledged by third parties.

e) shall not be responsible when the subject exceeds the limits set out in the certificate as to their possible uses, in accordance with the conditions laid down and communicated to the subject.

f) shall not answer if the recipient of the electronically signed documents does not prove them and takes into account the restrictions on the certificate as to their possible uses.

g) shall not assumes no responsibility in case of loss or damage:

- Of services provided in case of war, natural disasters or any other act of force majeure;
- Caused by the use of certificates when they exceed the limits established in the Certificate Policy and Certification Practice Statement;
- Caused by improper or fraudulent use of the certificates or CRL issued by it.

14. Agreements, Certification Practices Statement and Certification Policies

All applicable agreements, Certification Practice Statements, Certificate Policies and Privacy Policy are available at https://www.pki.globaltrustedsign.com/index.html.

15. Privacy Policy

The GTS CA implements measures that guarantee the privacy of personal data, in accordance with the Portuguese legislation, ensuring that the information of the subject, requested for the issuance of the respective qualified certificate, is not published and is processed in accordance with the Certificate Policies of the GTS CA.

16. Governing Law and Dispute Resolution

Any dispute arising from the interpretation or application of this document is ruled by Portuguese law. In order to regulate these disputes, the parties elect the Judicial District of Funchal as the dispute resolution jurisdiction, excluding any other.

17. Compensations

The GTS CA will assume its responsibility with respect to possible damages, in accordance with the applicable legislation in force.

18. Legislation and Standards

The GTS CA conducts its activity of issuing certificates according to the following rules/regulations:

- 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 of the European Parliament and of the Council of 13 December 1999, about an EU framework for electronic signatures);
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers, and the standards related to reliable services;
- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.2
- Other national and European legislation related to the provision of qualified trust services.

19. Audits and Security Standards

All interventions made to GTS CA are validated by internal auditors. GTS CA is audited by an independent auditor as required by the supervisory body. Its mission is to audit the infrastructure of the Certification Authority, regarding its technical and human resources, processes, policies and rules, having to submit an annual report to the supervisory body.

20. Acronyms

OSCP	*Online Certificate Status Protocol*
CRL	Certificate Revocation List
VPN	*Virtual Private Network*
CA	Certification Authority
DL	Decree Law
DCP	Disclosure of Certification Principles
EU	European Union