DISCLOSURE OF PRINCIPLES STATEMENT OF THE GTS TIMESTAMPING AUTHORITY

Global Trusted Sign

Document Reference | DP06_GTS_V6

TABLE OF CONTENTS

1. References	European Regulation Nº 910/2014 CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.5; RFC 3161 – Internet X.509 Public Key Infrastructure - Timestamp Protocol (TSP) ETSI 319 421 ETSI 319 422 ETSI 319 401
2. Related Documents	DP03_GTS – TSA Certification Practice Statement PL14_GTS – Timestamps Certificate Policy
3. Distribution List	Interested parties in the GTS trust hierarchy
4. Document History	31-07-2017 | Version 1 16-02-2018 | Version 2 01-06-2018 | Version 3 10-03-2020 | Version 4 24-06-2020 | Version 5 17-09-2020 | Version 6
5. Document Classification	D | Public

6. Revision

Version Number	Creation	Approval	Reason
	17-09-2020	**17-09-2020**	
	SegAdm	**Management Group**	
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
6	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 17-09-2020 17:42:20	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 17-09-2020 17:45:14	Update of GTS Trust Group and registrations.

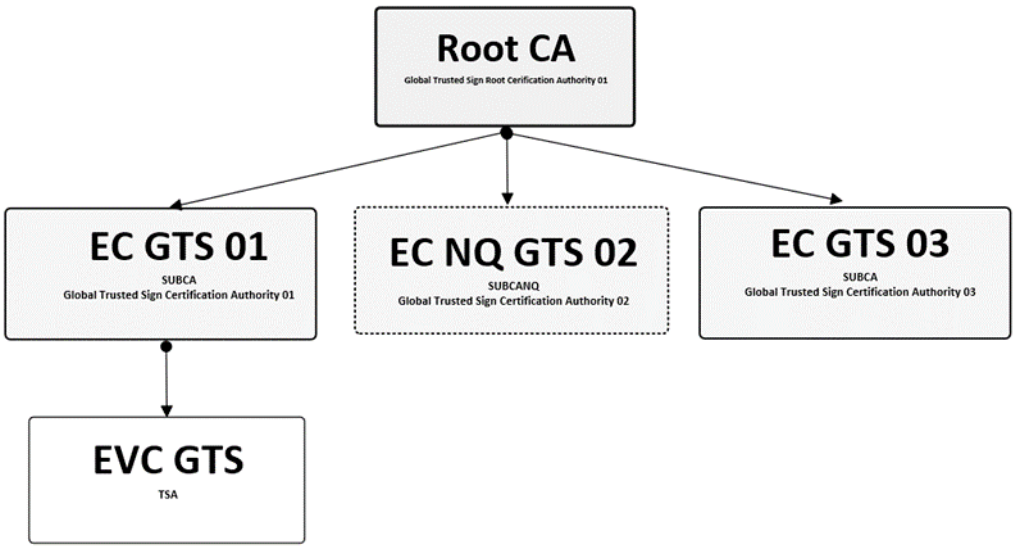
7. Introduction

7.1. Purpose

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

The infrastructure of the GTS TSA provides a trust hierarchy that promotes the electronic security of the digital certificate holder. The GTS TSA 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 TSA 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. The GTS TSA is signed by the ROOT CA GTS, 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 timestamp token subscribers issued by the GTS TSA.

7.3. Document Structure

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

This document is the Disclosure of Principles Statement of the Timestamping Authority of GTS, and its associated OID is: 1.3.6.1.4.1.50302.1.1.3.3.1.0, while the OID of good practices associated with the Timestamp Certificates Policy is 0.4.0.2023.1.1 (as stated by the ETSI EN 319 421 standard) and the unique identifier of the Timestamp Certificates Policy is 1.3.6.1.4.1.50302.1.1.2.3.1.0.

This document is identified by the information contained in the following table:

Document information	
Document Name	Disclosure of Principles Statement of the GTS Timestamping Authority
Document Version	6.0
Document Status	Approved
OID	1.3.6.1.4.1.50302.1.1.3.3.1.0
Issuance Date	17th September 2020
Validity	17th September 2021
Location	https://pki.globaltrustedsign.com/index.html

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

8. Contacts of the GTS Certification Authority

Name	GTS Timestamping 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

9. Types of Timestamps and Uses

The GTS TSA aims to deliver timestamping services used in support of qualified electronic signatures in accordance with the 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. The supported signing algorithm is sha256WithRSAEncryption (4096-bit key length)

Timestamps are issued at the request of the subscribers in accordance with the ETSI EN 319 421 standard and meet the requirements of the RFC 3161.

The TSU of the GTS TSA digitally signs the timestamp using digital certificates, each with a validity of five years. During this period and after the issuance of the timestamp, the validity of the timestamp can be verified, calculating the period between the date of issuance and the 5 years of validity.

10. Reliability Limits

The purpose of timestamps is to ensure that a document (or file) existed at a particular moment. This guarantee is obtained through the generation of a qualified timestamp issued by an accredited certifying authority (such as the GTS TSA) associated with the hash of the document to which the timestamp will be affixed.

This way, the association of a timestamp with the document certifies not only the veracity of the time and date of the request, but also the integrity and non-repudiation of the content.

Timestamps issued by the GTS TSA are reliable in the public context and comply with the following documents:

- GTS TSA Certification Practices Statement:
    - Defines the practices followed by the GTS TSA for certificate lifecycle management (OID: 1.3.6.1.4.1.50302.1.1.1.2.1.0)
- GTS TSA Certificate Policies: OID = 1.3.6.1.4.1.50302.1.1.2.7.1.0

The GTS TSA ensures that the clocks which provide the time/date (timestamp) included in the digital timestamp are synchronized with a precision of at least 1 second in relation to the UTC.

The GTS TSA logs are maintained for 7 years, and during this period are available as a supporting evidence of the accuracy indicated on issued timestamps.

11. Holders Responsibilities

Certificate holders shall use their private key only for the intended purposes (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 state) and is not in the CRL of the GTS TSA.

When using the certificate and its public key, the holder 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. Timestamping

12.1. Issuance of timestamps

Timestamps are issued in a safe manner and in accordance with the recommendations of ETSI EN 319 422 with a correct time/date (timestamp), having the following parameters:

- The identifier of the policy used to generate the timestamp (0.4.0.2023.1.1)
- A timestamp;
- A cryptographic hash of the data along with the timestamp;
- A unique serial number;
- An electronic seal generated with the GTS TSA private key, for this function;
- A minimum precision of 1 second in relation to the UTC, whose time synchronization of the GTS TSA is done with the time server provided by the Lisbon Astronomical Observatory (*Observatório Astronómico de Lisboa*).

12.2. Clock Synchronization

For the UTC synchronization required for the issuance of timestamps, an atomic clock with a GPS (Global Positioning System) connection is used. To satisfy the redundancy requirements imposed by the ETSI EN 319 412 standard, two other time sources have been configured as imposed by the same standard. The redundant sources of time considered are:

- Royal Observatory of Belgium (ORB), Brussels, Belgium - ntp1.oma.be
- Observatoire de Paris (LNE-SYRTE), Paris, France - ntp-p1.obspm.fr

12.3. Timestamp order processing

The subscriber submits the timestamp order, which is processed immediately and automatically by the TSA within the limits indicated in this document.

In case of loss of synchronism of the chronological validation services, the GTS TSA will not generate timestamps until the normal operating status is restored.

In case of compromise or suspicion of chronological validation services, the GTS TSA will not generate timestamps until the normal operating state is restored.

12.4. Proper use

Timestamps are issued at the request of subscribers and in accordance with the RFC 3161.

They are also used by Relying Parties for validation of the date/time association with the datum, and for this purpose they should:

- Verify that the timestamp has been correctly signed and that the private key used to sign the token has not been compromised until the time of verification. During the validity of the TSU certificate, the validity of the signing key can be verified by verifying the revocation status of the TSU certificate;
- Take into account the limitations on the use of the timestamp as defined in this practice statement and in the certificate policy;
- Take into account any other precautions applicable to the use of the timestamp defined, for example in agreements.

Note: The requirements and rules defined in this document apply to all timestamps issued by the GTS TSA.

12.5. Unauthorized use

Timestamps cannot be used for any function other than the uses described in the previous section and applicable legislation.

13. Limitations and Responsibilities

The GTS TSA:

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

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

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

g) shall not assume any 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://pki.globaltrustedsign.com/index.html.

15. Privacy Policy

The GTS TSA implements measures that guarantee the privacy of personal data, in accordance with the General Data Protection Regulation (Reg. 2016/679), ensuring that the information of the holder, requested for the issuance of the respective timestamps, is not disclosed, and it is processed in accordance with the GTS TSA Privacy Policy.

16. Governing Law and Dispute Resolution

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

17. Compensations

The GTS TSA shall assume responsibility with respect to possible damages, in accordance with the applicable legislation in force.

18. Legislation and Standards

The GTS TSA conducts its activity of issuance of 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, on a Community 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 the GTS Certification Authority are validated by internal auditors. The GTS TSA is audited by an independent auditor as required by the Supervisory Body. His/her purpose is to audit the infrastructure of the Timestamping 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