TIMESTAMP CERTIFICATE POLICY

Global Trusted Sign

Document Reference | PL14_GTS_V8
Document Classification: Public
Date: 06th may 2021

Table of Contents

1. Introduction

Purpose

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

Target Audience

This document should be read by:

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

Document Structure

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

1.1 Overview

This document focuses on the definition of profiles of Timestamp Certificates issued the GTS TSA (Global Trusted Sign Timestamping Authority), enabling the assurance of liability of the Chronological Validation also available in the GTS PKI. The certificates issued by the GTS TSA contain a reference to the GTS TSA Certification Practice Statement (TSA CPS) in order to allow relying parties and other interested entities or persons to find information about the certificate and the policies followed by the issuing authority.

1.2 Document Name and Identification

This document is the "Timestamp Certificate Policy". This Certificate Policy (CP) is represented on a certificate through a unique number referred to as "Object Identifier" (OID).

Document information	
Document Version	8
Document Status	Approved
OID "Object Identifier"	1.3.6.1.4.1.50302.1.1.2.3.1.0
Issuance date	06th may 2021
Validity	06th may 2022
Location	https://pki.globaltrustedsign.com/index.html

1.2.1 Revision Record

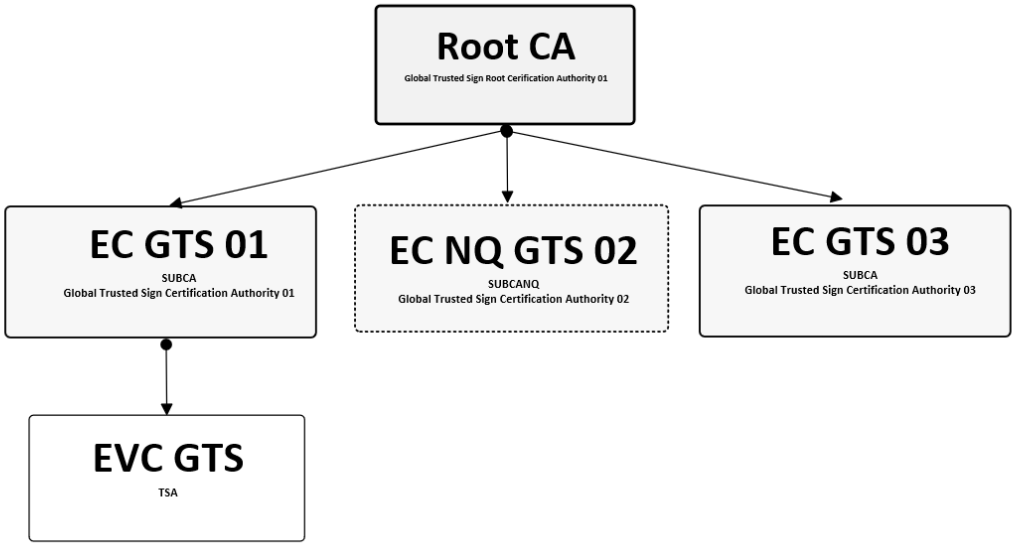
Version Number	Creation	Approval	Reason
	06-05-2021	**06-05-2021**	
8	**Security Administration**	**Group Management**	Update of document structure according to RFC 3647
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 06-05-2021 16:05:35	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 06-05-2021 16:12:38	

1.2.2 Relevant Dates

Version ID	Version Date	Reason for new version
Version 1	14-08-2017	To present the Timestamp Certificate Policy of the Global Trusted Sign Timestamping Authority, as a qualified service provider under regulation 910/2014
Version 2	13-02-2018	Update of the certificate "O" field
Version 3	26-07-2018	Update of OID validity
Version 4	10-01-2019	Update of OID validity
Version 5	31-01-2019	Update of the certificate attributes
Version 6	06-03-2020	Update of OID
Version 7	17-09-2020	Update of registration of employees of the GTS Trust Group
Version 8	06-05-2021	Update of document structure according to RFC 3647

1.3. PKI Participants

GTS, as a qualified trust service provider, has a trust hierarchy accredited by the National Security Office (http://www.gns.gov.pt/trusted-lists.aspx), in accordance with the Portuguese and European legislation. The GTS trust hierarchy has a group of devices, applications, human resources and procedures required to implement diverse available certification services and to ensure the life cycle of certificates described in this document. The GTS trust hierarchy is composed by the GTS Root Certification Authority (GTS ROOT CA), the GTS Certification Authorities (GTS CA01 and GTS CA03), the GTS Non-qualified Certification Authority (GTS NQ CA) and the GTS Timestamping Certification Authority (GTS TSA CA). These Certification Entities are described in sections 1.3.1.1, 1.3.1.2, 1.3.1.3 and 1.3.1.4, of this document, and are illustrated as follows:



Legend:

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

1.4. Certificate Usage

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

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

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

1.5. Policy Administration

1.5.1. Organization Administering the Document

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

1.5.2. Contact Entity

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

Tel: 707 451 451 / + 351 291 957 888

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

1.6. Definitions and Acronyms

1.6.1. Definitions

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

Definitions	
Term	**Definition**
Electronic Seal Creation Data	Unique group of data used by the creator of the e-seal to create an e-seal.
Electronic Signature Creation Data	Unique group of data used by the signatory to create an electronic signature.
Electronic Signature Creation Device	Configured *software* or *hardware*, used to create an electronic signature
Electronic Seal Creation Device	Configured *software* or *hardware* used to create an electronic seal.
Qualified Electronic Signature Creation Device	Electronic signature creation device that meets the requirements laid down in Annex II of the European Regulation 910/2014.
Qualified Electronic Seals Creation Device	Electronic seal creation device that meets *mutatis mutandis* the requirements laid down in Annex II of the European Regulation 910/2014.
Electronic Document	Any content stored in electronic form, in particular text or sound, visual or audio-visual recording.
Electronic Address	Identification of computer equipment, proper to receive and file electronic documents.
Certification Authority	Natural or legal person, accredited as a qualified service provider by the supervisory authority.
Registration Authority	Entity that approves Distinct Names (DN) of subordinated entities and, by assessing the request, approves or rejects the request.
Supervisory Authority	Appointed entity for the accreditation and inspection of certification authorities.
Hash Function	Operation done by a group of data in any size, so that the result is another fixed size group of data independent from its original size and is uniquely linked to initial data and ensures it is impossible to obtain distinct messages that manage the result when applying that function.
Hash or Fingerprint	Fixed size result obtained after the application of a hash function to a message that complies the requirement of being uniquely linked to initial data.
HSM	Cryptographic security module used to store keys and cryptographic operations in a secure way.
Electronic Identification	The process of using personal identification data in electronic form, representing uniquely either a natural or legal person, or a natural person representing a legal person.
Public Key Infrastructure	Hardware, software, persons, processes and policies structure that uses digital signature technology to provide trusted third parties a verifiable association between the public component of an asymmetric pair of keys and a specific signatory.
CRL	Revoked certificates list created and signed by the Certification Authority (CA) that issued the certificates. A certificate is introduced on the list when has been revoked (for example, by suspecting the key's compromise). In certain circumstances, the CA can divide a CRL into smaller CRLs.
Electronic Identification Mean	A material and/or immaterial unit containing personal identification data and which is used for authentication for an online service.
OID	Unique alphanumeric/numeric identifier registered according to an ISO norm, to refer to a specific object or to a specific class of objects.
Conformity Assessment Body	A body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides.

Definitions	
Term	**Definition**
Public Body	National, regional or local government body, a body subject to public law or an association formed by one or more of those entities or by a body subject to public law, or a private entity authorised by, at least, one of those authorities, bodies or associations as being of public interest, under the current mandate.
Relying Party	Relying parties or final recipients are natural or legal people that trust in the validity of mechanisms and procedures used in the linking process of a time stamp to a datum. In other words, they rely on the time stamp's accuracy.
Certificate Policy	Group of rules that indicate the certificate's applicability to a specific community and/or application class with common security requirements.
Trust Service Provider	Natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
Qualified Trust Service Provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Product	Hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services.
Electronic Seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
Advanced Electronic Seal	Electronic seal which meets the following requirements: a) it is uniquely linked to the creator of the seal b) it is capable of identifying the creator of the seal c) it is created using e-seal creation data that the creator of the seal can, with a high level of confidence under its control, use for e-seal creation; and d) d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
Qualified Electronic Seal	Advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.
Qualified Timestamp	An electronic timestamp which meets following requirements: a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably b) it is based on an accurate time source linked to Coordinated Universal Time; and c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.
Timestamps	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
Trust Service	Electronic service normally provided for remuneration which consists of: a) the creation, verification, and validation of electronic signatures, e-seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or b) the creation, verification and validation of certificates for website authentication; or c) the preservation of electronic signatures, seals or certificates related to those services.
Qualified Trust Service	Trust service that meets the applicable requirements laid down in the European Regulation 910/2014.

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

1.6.2. Acronyms

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

1.6.3. References

- ✓ DP03_GTS – GTS Timestamp Authority Certification Practice Statement.
- ✓ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- ✓ ETSI 319 421 Electronic Signatures and Infrastructures (ESI) Policy and Security Requirements for Trust Service Providers Issuing Time Stamps;
- ✓ ETSI 319 422 Electronic Signatures and Infrastructures (ESI) Time-stamping protocol and time-stamp token profiles;
- ✓ RFC 3161 – Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP);
- ✓ RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;
- ✓ CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.7.4.

2. Publication and Repository Responsibilities

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

3. Identification and Authentication

3.1. Naming

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

3.1.1. Types of Names

The GTS TSA certificate is identified by a Distinguished Name (DN), according to what is set in standard X.509. The unique name of the timestamp certificate is identified by the following components:

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

3.2. Certificate and Key Pair Usage by the Subscriber

GTS is the holder of the Timestamp Certificate issued for the GTS PKI Timestamping Authority (TSA). The private key associated to this type of certificates is used to sign the responses to chronological validation requests (timestamping), guaranteeing and allowing the verification of integrity and non-repudiation of these same responses.

4. Certificate Profile

4.1. Certificate Profile

The Timestamp certificate profile complies with ETSI 319 412 and ETSI 319 422 standards.

4.1.1. Version Number

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

4.1.2. Certificate Content and Extensions; Application of RFC 5280

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

4.1.2.1. Profile of the Timestamping Authority Certificate

Certificate Component	Value	Type	Remarks
Version	V3	M	
Serial Number	<Assigned by the CA to each certificate>	M	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Certificate's signature. The value must be equal to the OID of the *SignatureAlgorithm* (below)
Issuer		M	
Country (C)	"PT"		Country of the issuing authority
Organization (O)	"ACIN iCloud Solutions, Lda"		Name of the organization of the issuing authority

Certificate Component	Value	Type	Remarks
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Certification Authority 01		
Validity			Validity of the Certificate
Valid from	<Date of issuance>		
Valid to	<Date of issuance + 5 years>		5-year maximum validity
Subject		M	
Country (C)	PT		Nationality of the certificate's holder
Organization (O)	ACIN iCloud Solutions, Lda		
Organization Unit (OU)	Global Trusted Sign		
Common Name (CN)	Global Trusted Sign Timestamping Authority 001		
Subject Public Key Info		M	
Algorithm	rsaEncryption (OID: 1.2.840.113549.1.1.1)		Public key algorithm
subjectPublicKey	<Public Key>		Certificate public key
Authority Key Identifier		M	
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	Certificate key identifier
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		
Enhanced Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)		
Certificate Policies		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.1.3.1.0 Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identifier and location of the GTS TSA Certification Practice Statement

Certificate Component	Value	Type	Remarks
[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 of 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 Certification Revocation List
[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_subca_crl.crl		Secondary location of the GTS SUBCA Certification Revocation List
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Algorithm used to create the signature of the certificate
Signature Value	<It contains the digital signature issued by the CA>	M	Signature of the certificate

4.1.3. Algorithm Object Identifiers

The certificate "*signatureAlgorithm*" field contains the OID of the cryptographic algorithm used by the GTS CA to sign the certificate (1.2.840.113549.1.1.11 - sha256WithRSAEncryption).

4.1.4. Name Forms

See section 3.1.1.

4.1.5. 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.

4.1.6. Certificate Policy Object Identifier

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

4.1.7. Usage of Policy Constraints Extensions

No stipulation.

4.1.8. 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*" extension, which contains a pointer, in the form of a URL, to the Certificate Policy.