POLÍTICA DE CERTIFICADOS DE SELOS TEMPORAIS

Global Trusted Sign

Referência do Documento | PL14_GTS_V8
Classificação do Documento: Público
Data: 06 de maio de 2021

Índice

1. Introdução

Objetivo

O objetivo deste documento é apresentar a Política de Certificados de Selos Temporais da Entidade de Validação Cronológica da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014 adiante designada por EVC GTS.

Público Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EVC GTS;
- Terceiras partes, encarregues de auditar a EVC GTS;
- Todo o público, em geral

Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave-pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focados antes de proceder com a leitura do documento. Não se pretende nomear as regras legais ou obrigações, mas antes informar, pelo que se pretende que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais

1.1 Contexto Geral

O presente documento define os perfis dos Certificados de validação cronológica emitidos pela EVC GTS (Entidade de Validação Cronológica da Global Trusted Sign), permitindo assim garantir a fiabilidade da Validação Cronológica disponível também na PKI GTS. Os certificados emitidos pela EVC GTS contêm uma referência à Declaração de Práticas de Certificação da EVC GTS de modo a permitir que partes confiantes e outras entidades ou pessoas interessadas possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

1.2 Designação e Identificação do Documento

Este documento é a "Política de Certificados de Selos Temporais". Esta Política de Certificado (PC) é representada num certificado através de um número único designado de "identificador de objeto" (OID).

Informação do Documento	
Versão do Documento	8
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.2.3.1.0
Data de Emissão	06 de maio de 2021
Validade	06 de maio de 2022
Localização	https://pki.globaltrustedsign.com/index.html

1.2.1 Registo de Revisão

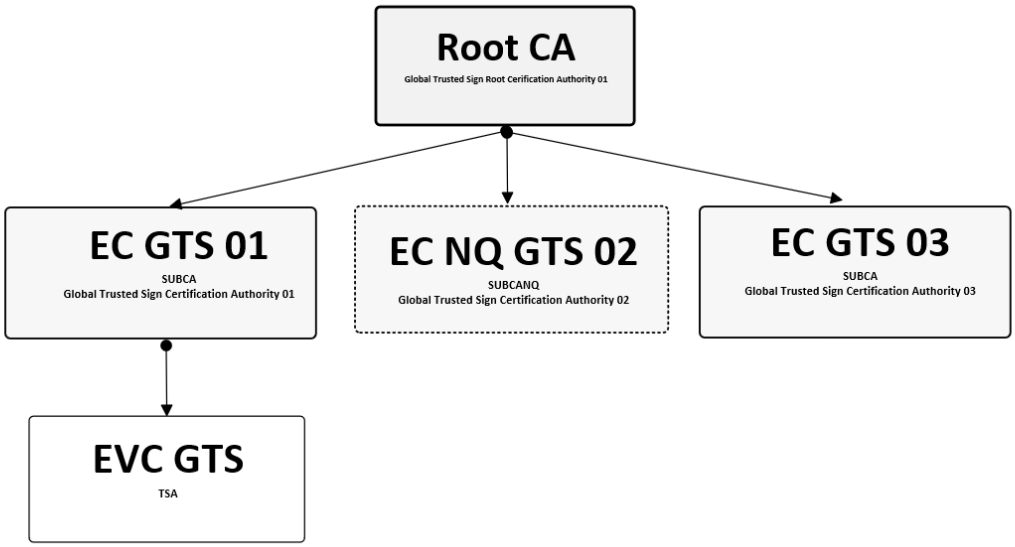
N.º da Versão	Elaborado	Aprovado	Motivo
	06-05-20201	06-05-2021	
7	**AdmSeg**	**Grupo de Gestão**	Atualização de estrutura do documento, de acordo com o RFC 3647
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 06-05-2021 16:29:11	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 06-05-2021 16:30:29	

1.2.2 Datas relevantes

ID de versão	Data da versão	Motivo de nova versão
Versão 1	14-08-2017	Apresentar a Política de Certificados de Selos Temporais da Entidade de Validação Cronológica da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014
Versão 2	13-02-2018	Atualização do Campo "O" do certificado
Versão 3	26-07-2018	Atualização de validade do OID
Versão 4	10-01-2019	Atualização de validade do OID
Versão 5	31-01-2019	Atualização dos atributos do certificado
Versão 6	06-03-2020	Atualização do OID
Versão 7	17-09-2020	Atualização de registo de colaboradores do Grupo de Confiança da GTS
Versão 8	06-05-2021	Atualização de estrutura do documento, de acordo com o RFC 3647

1.3. Participantes na Infraestrutura de Chave Pública

A GTS, enquanto prestador qualificado de serviços de confiança, disponibiliza uma hierarquia de confiança credenciada pelo Gabinete Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), conforme previsto na legislação portuguesa e europeia. É composta por um conjunto de equipamentos, aplicações, recursos humanos e procedimentos indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir assim a adequada gestão do ciclo de vida dos certificados descritos no presente documento. A hierarquia de confiança da GTS é composta pela Entidade Certificadora Raiz da GTS (ROOT CA GTS), as Entidades Certificadoras da GTS (EC GTS01 e EC GTS03), a Entidade Certificadora Não Qualificada da GTS (EC NQ GTS) e a Entidade Certificadora de Selos Temporais da GTS (EVC GTS). Estas entidades certificadoras estão descritas nos pontos 1.3.1.1, 1.3.1.2, 1.3.1.3 e 1.3.1.4 do presente documento e encontram-se ilustradas de seguida:



Legenda:

1 – Root CA GTS **- Entidade Certificadora Raiz da GTS**
2 – EC GTS 01 **– Entidade Certificadora da GTS**
3 – EC NQ GTS 02 **– Entidade Certificadora Não Qualificada da GTS**
4 – EVC GTS **– Entidade Certificadora de Validação Cronológica da GTS**
5 – EC GTS 03 **– Entidade Certificadora da GTS**

1.4. Utilização do Certificado

Os certificados emitidos pelo PKI da GTS são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança, nomeadamente:

- Autenticação;
- Confidencialidade;
- Integridade;
- Privacidade de Dados;
- Não Repúdio;
- Autenticidade.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, mediante a utilização da estrutura de confiança que a PKI da GTS disponibiliza. As Partes Confiantes podem verificar a cadeia de confiança de um certificado emitido pela EC GTS, garantindo assim a autenticidade e identidade do titular. Os certificados qualificados emitidos pela EC GTS estão de acordo com esta DPC e são certificados qualificados em conformidade com os requisitos do regulamento (EU) 910/2014.

1.5. Gestão de Políticas

1.5.1. Entidade Responsável pela Gestão do Documento

A gestão desta declaração de práticas de certificação da EC GTS é da responsabilidade do grupo de Confiança da GTS.

1.5.2. Entidade de Contato

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. Definições e Acrónimos

1.6.1. Definições

Definições	
Termo	**Definição**
Assinatura Eletrónica	Dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar
Assinatura Eletrónica Avançada	Assinatura eletrónica que obedeça aos requisitos: a) Esteja associada de modo único ao signatário b) Permita identificar o signatário c) Seja criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo, e d) Esteja ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados
Autenticação	Processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar
Certificado	Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.
Certificado de Assinatura Eletrónica	Atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo
Certificado de Autenticação de Sítio Web	Atestado que torne possível autenticar um sítio web e associe o sítio web à pessoa singular ou coletiva à qual o certificado tenha sido emitido
Certificado de Selo Eletrónico	Atestado eletrónico que associa os dados de validação do selo eletrónico a uma pessoa coletiva e confirma o seu nome
Certificado Qualificado de Assinatura Eletrónica	Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Autenticação de Sítios Web	Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Selo Eletrónico	Certificado de selo eletrónico emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III do Regulamento europeu 910/2014
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves
Credenciação	Ato pelo qual é reconhecido a um prestador de serviços que o solicite e que exerça a atividade de entidade certificadora em conformidade com os requisitos definidos no Regulamento europeu 910/2014
Criador de um Selo	Pessoa coletiva que cria um selo eletrónico
Dados de Identificação Pessoal	Conjunto de dados que permita determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa coletiva
Dados de Validação	Dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico

Definições	
Termo	**Definição**
Dados para a Criação de um Selo Eletrónico	Conjunto único de dados que seja utilizado pelo criador do selo eletrónico para criar um selo eletrónico
Dados para a Criação de uma Assinatura Eletrónica	Conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica
Dispositivo de Criação de Assinaturas Eletrónicas	*Software* ou *hardware* configurados, utilizados para criar assinaturas eletrónicas
Dispositivo de Criação de Selos Eletrónicos	*Software* ou *hardware* configurados, utilizados para criar selos eletrónicos
Dispositivo Qualificado de Criação de Assinaturas Eletrónicas	Dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Dispositivo Qualificado de Criação de Selos Eletrónicos	Dispositivo para a criação de selos eletrónicos que satisfaça *mutatis mutandis* os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Documento Eletrónico	Qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Entidade Certificadora	Entidade ou pessoa singular ou coletiva credenciada como prestador qualificado de serviços de confiança pela entidade supervisora
Entidade de Registo	Entidade que aprova os Nomes Distintos (DN) das entidades subordinadas e, mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo
Entidade Supervisora	Entidade competente para a credenciação e fiscalização das entidades certificadoras
Função Hash	Operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função.
Hash ou Impressão Digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais
HSM	Módulo de segurança criptográfico empregue para armazenar chaves e realizar operações criptográficas de modo seguro
Identificação Eletrónica	O processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva
Infraestrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas
Meio de Identificação Eletrónica	Uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha
OID	Identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica

Definições	
Termo	**Definição**
Organismo de Avaliação da Conformidade	Organismo definido que é acreditado nos termos do regulamento 910/2014 como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados
Organismo Público	Entidade estatal nacional, regional ou local, um organismo de direito público ou uma associação formada por uma ou mais dessas entidades ou por um ou mais organismos de direito público, ou uma entidade privada mandatada por, pelo menos, uma dessas autoridades, organismos ou associações como sendo de interesse público, ao abrigo de tal mandato
Parte Confiante	As partes confiantes ou destinatários são pessoas singulares ou entidades que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação de um selo temporal ao datum, ou seja, confiam na veracidade do selo temporal.
Política de Certificado	Conjunto de regras que indica a aplicabilidade do certificado a uma comunidade específica e/ou classe de aplicação com requisitos de segurança comuns
Prestador de Serviços de Confiança	Pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança
Prestador Qualificado de Serviços de Confiança	Prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora
Produto	*Hardware* ou *software*, ou componentes pertinentes de hardware ou software, que se destinem a ser utilizados para a prestação de serviços de confiança
Selo Eletrónico	Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos
Selo Eletrónico Avançado	Selo eletrónico que obedeça aos requisitos: a) Esteja associado de modo único ao seu criador b) Permita identificar o seu criador c) Seja criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico, e d) Esteja ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dados
Selo Eletrónico Qualificado	Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico
Selo Temporal Qualificado	Selo temporal que satisfaça os requisitos: a) Vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável, b) Basear-se numa fonte horária precisa ligada à Hora Universal Coordenada, e c) Ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente
Selos Temporais	Dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento

Definições	
Termo	**Definição**
Serviço de Confiança	Serviço eletrónico geralmente prestado mediante remuneração, que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços, ou b) Na criação, verificação e validação de certificados para a autenticação de sítios web, ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços
Serviço de Confiança Qualificado	Serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento europeu 910/2014
Serviço de Envio Registado Eletrónico	Serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada
Serviço Qualificado de Envio Registado Eletrónico	Serviço de envio registado eletrónico que satisfaça os requisitos: a) Serem efetuados por um ou mais prestadores qualificados de serviços de confiança b) Garantirem, com um elevado nível de confiança, a identificação do remetente c) Garantir a identificação do destinatário antes da entrega dos dados d) O envio e a receção dos dados serem securizados por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, de modo a tornar impossível a alteração dos dados de forma não detetável e) Qualquer alteração a que devam ser sujeitos para o seu envio ou receção ser claramente indicada ao remetente e ao destinatário dos dados f) A data e a hora do envio e da receção, assim como as eventuais alterações dos dados, serem indicadas por meio de um selo temporal qualificado
Signatário	Pessoa singular que cria uma assinatura eletrónica.
Sistema de Identificação Eletrónica	Sistema de identificação eletrónica ao abrigo do qual sejam produzidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem pessoas coletivas
Titular	Ver Signatário.
Utilizador	Pessoa singular ou coletiva que utiliza a identificação eletrónica ou o serviço de confiança
Validação	Processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico
Validação Cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos

1.6.2. Acrónimos

Acrónimos	
C	*Country*
CN	*Common Name*
DN	Nome Distinto *(Distinguished Name)*
DPC	Declaração de Práticas de Certificação
DR	Decreto Regulamentar
EC	Entidade Certificadora
ER	Entidade de Registo
GNS	Gabinete Nacional de Segurança
GTS	*Global Trusted Sign*
HSM	Modulo Criptográfico em Hardware (*Hardware Secure Module*)
LRC	Lista de Revogação de Certificados
O	*Organization*
OU	*Organization Unit*
OID	Identificador de Objeto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	Infraestrutura de Chave Pública *(Public Key Infrastructure)*
SSL/TLS	*Secure Sockets Layer / Transport Layer Security*

1.6.3. Referências Bibliográficas

- ✓ DP03_GTS - Declaração de Práticas de Certificação da Entidade de Validação Cronológica.
- ✓ Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- ✓ 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. Responsabilidade de Publicação e Repositório

O repositório das diversas entidades certificadoras pode ser acedido 24x7 em:
https://pki.globaltrustedsign.com/index.html
https://pki02.globaltrustedsign.com/index.html
O repositório será atualizado sempre que haja uma alteração num dos documentos publicados.

3. Identificação e Autenticação

3.1. Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela Declaração de Práticas de Certificação.

3.1.1. Tipos de Nomes

O certificado da EVC GTS é identificado por um nome único (DN – Distinguished Name) de acordo com o standard X.509. O nome único do certificado de validação cronológica é identificado pelos seguintes componentes:

Atributo	Código	Valor
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. Uso do certificado e par de chaves pelo titular

A GTS é a titular do Certificado de Validação Cronológica, sendo o mesmo emitido para a Entidade de Validação Cronológica (EVC) da PKI da GTS. A chave privada associada a este tipo de certificados é utilizada para assinar as respostas a pedidos de validações cronológicas (aposição de selos temporais), garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

4. Perfil de Certificado

4.1. Perfil de Certificado

O perfil do certificado de Selo Temporal está de acordo com o conjunto de standards ETSI 319 412 e ETSI 319 422.

4.1.1. Número da Versão

O campo ***version*** do certificado descreve a codificação utilizada no certificado, sendo a versão 3 a versão utilizada (V3).

4.1.2. Extensões do Certificado

Os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

4.1.2.1. Perfil de Certificado da Timestamping Authority

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<Atribuído pela EC a cada certificado>	M	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado. Valor tem que ser igual ao OID no *SignatureAlgorithm* (abaixo)
Issuer		M	
Country (C)	"PT"		País da entidade emissora
Organization (O)	"ACIN iCloud Solutions, Lda"		Designação da organização da entidade emissora

Componente do Certificado	Valor	Tipo	Comentários
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Certification Authority 01		
Validity			Validade do Certificado
Valid from	<data de emissão>		
Valid to	<data de emissão + 5 anos>		Validade máxima de 5 anos
Subject		M	
Country (C)	PT		País de nacionalidade do titular do certificado
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)		Algoritmo de chave pública
subjectPublicKey	<Chave Pública>		Chave pública do certificado
Authority Key Identifier		M	
keyIdentifier	160 bit hash		Permite identificar a chave pública correspondente à chave privada do certificado
Subject Key Identifier	160 bit hash	M	Identificador da chave do certificado
Key Usage		M	
Digital Signature	"1" selecionado		
Non Repudiation	"1" selecionado		
Key Encipherment	"0" selecionado		
Data Encipherment	"0" selecionado		
Key Agreement	"0" selecionado		
Key Certificate Signature	"0" selecionado		
CRL Signature	"0" selecionado		
Encipher Only	"0" selecionado		
Decipher Only	"0" selecionado		
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		Identificador e localização da Declaração de Práticas de Certificação da EVC GTS

Componente do Certificado	Valor	Tipo	Comentários
[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 Identificador e localização na política de Certificados de Selos Temporais
Basic Constraints		M	
Subject Type	End Entity	C	Certificado destinado o Timestamping
PathLenConstraint	None		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_subca_crl.crl		Localização da Lista de Revogação de Certificados da SUBCA GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_subca_crl.crl		Localização secundária da Lista de Revogação de Certificados da SUBCA GTS
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Algoritmo usado para a criação da assinatura do certificado
Signature Value	<contém a assinatura digital emitida pela CA>	M	Assinatura do certificado

4.1.3. OID do Algoritmo

O campo *"signatureAlgorithm"* do certificado contém o OID do algoritmo criptográfico utilizado pela EVC GTS para assinar o certificado (1.2.840.113549.1.1.11 - sha256WithRSAEncryption).

4.1.4. Formatos de Nome

Consultar ponto 3.1.1.

4.1.5. Condicionamento dos Nomes

Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se (mas não se obriga) a que apenas caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') sejam utilizados em entradas do Diretório X.500.

4.1.6. OID da Política de Certificado

Todos os certificados emitidos pela PKI GTS contêm os seguintes qualificadores: "*policyQualifIierID*= CPS" e "*cPSuri*", que aponta para o URL onde se encontra a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*".

4.1.7. Utilização de Extensão de Restrições de Política

Não estipulado.

4.1.8. Sintaxe e Semânticas de Qualificadores de Política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores de certificados e autores da política de certificado. O tipo de qualificador é o "*CPSuri*", que contém um apontador, na forma de URL, para a Declaração de Práticas de Certificação publicada pela EC; e o "*userNotice explicitText*", que contém um apontador, na forma de URL, para a Política de Certificado.