POLÍTICA DE CERTIFICADOS DE SELOS TEMPORAIS

Global Trusted Sign

Referência do Documento | PL14_GTS_V7

ÍNDICE

1. Referências	Regulamentação Europeia Nº 910/2014 CA-Browser-Forum-BR-1.6.7 ETSI 319 421 ETSI 319 422
2. Documentos Associados	PC04_GTS - Processo de Emissão de Selos Temporais FO22_GTS - Formulário de pedido de Selos Temporais PR28_GTS - Procedimento de inativação de Pacote de Selos Temporais DP03_GTS - Declaração de Práticas de Certificação da EVC GTS DP06_GTS - PKI Disclosure Statement TSA GTS - EN
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	14-08-2017 | Versão 1 13-02-2018 | Versão 2 26-07-2018 | Versão 3 10-01-2019 | Versão 4 31-01-2019 | Versão 5 06-03-2020 | Versão 6 17-09-2020 | Versão 7
5. Classificação do Documento	D | Público

6. Registo da Revisão

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	06-03-2020	**06-03-2020**	
7	**AdmSeg**	**Grupo de Gestão**	Atualização de registo de colaborador do Grupo de Confiança da GTS
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	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 17:45:15	

7. Introdução

7.1. 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).

7.2. 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.

7.3. Estrutura do Documento

É recomendado que o leitor tenha conhecimentos sobre os conceitos de criptografia, infraestruturas de chave-pública e assinatura eletrónica. Caso esta situação não se verifique propõe-se o aprofundar os conceitos e os conhecimentos sobre os tópicos anteriormente mencionados.

8. Contexto Geral

O objetivo do presente documento é a definição dos 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. 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.

Os certificados emitidos pela EVC GTS contêm uma referência à Declaração de Práticas de Certificação da EVC GTS (DPVC) 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.

8.1. Visão Geral

Esta Política de Certificação satisfaz e complementa os requisitos definidos na Declaração de Práticas de Certificação da EVC GTS.

8.2. 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).

Este documento é identificado pelos dados constantes na seguinte tabela:

Informação do Documento	
Versão do Documento	7
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.2.3.1.0
Data de Emissão	17 de setembro de 2020
Validade	17 de setembro de 2021
Localização	https://pki.globaltrustedsign.com/index.html

9. Identificação e Autenticação

9.1. Atribuição de Nomes

A atribuição de nomes segue a seguinte convenção:

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

9.1.1. Tipos de nomes

O certificado da EVC GTS é identificado por um nome único (DN – Distinguished Name) de acordo com o standard X.509.

10. Perfis de Certificado

10.1. 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.

10.1.1. Número da Versão

O campo “version” do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é 3 (V3).

10.1.2. Extensões do Certificado

As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

10.1.3. 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
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

Componente do Certificado	Valor	Tipo	Comentários
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
[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

Componente do Certificado	Valor	Tipo	Comentários
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

10.1.4. OID do Algoritmo

O campo “signatureAlgorithm” do certificado contém o OID do algoritmo criptográfico utilizado pela Root GTS para assinar o certificado da Timestamping Authority. O algoritmo usado é sha256WithRSAEncryption que tem o OID 1.2.840.113549.1.1.11.

10.1.5. Condicionamento nos 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.

10.1.6. Utilização da extensão Policy Constraints

Não aplicável.