

# **POLÍTICA DE CERTIFICADOS PARA AUTENTICAÇÃO DE SÍTIOS WEB (SSL ORGANIZATION VALIDATION)**

---

Global Trusted Sign

Referência do Documento | PL04\_GTS\_V6

## ÍNDICE

1. Referências	3
2. Documentos Associados	3
3. Lista de Distribuição	3
4. Histórico do Documento	3
5. Classificação do Documento	3
6. Registo da Revisão	3
7. Introdução	4
8. Contexto Geral	4
9. Identificação e Autenticação	5
9.1. Atribuição de Nomes	5
9.2. Uso do Certificado e par de chaves pelo titular	5
10. Perfis de Certificado	6
10.1. Perfil de certificado	6
10.1.1. Número da versão	6
10.1.2. Extensões do Certificado	6
10.1.3. Emissão de Certificados de Autenticação de Sítios Web	7
10.1.4. OID do Algoritmo	11
10.1.5. Condicionamento nos Nomes	11
10.1.6. OID e sintaxe da Política de Certificados	11
10.1.7. Utilização de extensão Policy Constraints	11

<b>1. Referências</b>	Regulamento 910/2014   45.1; Anexo IV ETSI EN 319 411-1   6.6.3; 6.2.3; 6.3.7 ETSI EN 319 411-2   6.6.3; 6.2.3; 6.3.7 BRG CA/Browser Forum   6.1.6; 6.1.7; 7.1
<b>2. Documentos Associados</b>	PC03_GTS - Processo de Emissão de Certificados para Autenticação de Sítios Web PC15_GTS - Processo de Revogação de Certificados para Autenticação de Sítios Web DP02_GTS - Declaração de Práticas de Certificação da EC GTS DP02_GTS - Declaração de Práticas de Certificação da EC GTS
<b>3. Lista de Distribuição</b>	Partes interessadas da hierarquia de confiança da GTS
<b>4. Histórico do Documento</b>	31-07-2017   Versão 1 18-08-2017   Versão 2 25-08-2017   Versão 3 31-01-2019   Versão 4 09-03-2020   Versão 5 04-11-2020   Versão 6
<b>5. Classificação do Documento</b>	D   Público

## 6. Registo da Revisão

N.º da Versão	Elaborado	Aprovado	Motivo
	04-11-2020	04-11-2020	
6	<b>AdmSeg</b>	<b>Grupo de Gestão</b>	Atualização de AdmSeg
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	

## 7. Introdução

O presente documento tem como objetivo apresentar a Política de Certificados para autenticação de Sítios Web (SSL Organization Validation) da Entidade Certificadora da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014 (adiante designada por EC GTS).

O presente documento apresenta-se disponível publicamente e é destinado a todos os participantes que se relacionem, de alguma forma, com a Entidade Certificadora da GTS.

No âmbito da presente declaração de práticas assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica.

## 8. Contexto Geral

O objetivo do presente documento é a definição do perfil dos Certificados de Autenticação de Sítios Web (SSL Organization Validation) emitidos pela EC GTS (Entidade de Certificação da Global Trusted Sign).

Os certificados emitidos pela EC GTS contêm uma referência à Declaração de Práticas de Certificação da EC GTS (DPC), sendo a DPC completada pela presente Política de Certificação.

O presente documento designa-se "Política de Certificados para Autenticação de Sítios Web (SSL Organization Validation)".

<b>Informação do Documento</b>	
<b>Versão do Documento</b>	6
<b>Estado do Documento</b>	Aprovado
<b>OID</b>	1.3.6.1.4.1.50302.1.1.1.2.1.1
<b>Data de Emissão</b>	04 de novembro de 2020
<b>Validade</b>	04 de novembro de 2021
<b>Localização</b>	<a href="https://pki.globaltrustedsign.com/index.html">https://pki.globaltrustedsign.com/index.html</a>

## 9. Identificação e Autenticação

### 9.1. Atribuição de Nomes

A atribuição de nomes segue a convenção:

Atributo	Código	Valor
Country	C	<País>
Locality Name	L	<Localidade>
Organization	O	<Nome da Organização>
Common Name	CN	<Fully Qualified Domain Name do Servidor Web >

### 9.2. Uso do certificado e par de chaves pelo titular

A EC GTS é uma entidade emissora de certificados para sítios web. O nome qualificado do domínio do serviço ou sítio web está contido campo Common Name do certificado, sendo este certificado usado para o estabelecimento de uma ligação segura SSL/TLS.

## 10. Perfis de Certificado

### 10.1. Perfil de Certificado

O par de chave pública – chave privada está associado a um titular cujo principal uso é a utilização mecanismos de cifra e assinatura digital. O utilizador da chave pública confia na respetiva chave privada sendo esta confiança dada através do uso de certificados digitais X.509 v3 (fazendo uma ligação do titular com chave pública). A EC GTS assina digitalmente o certificado digital, certificando-se que o titular possui a chave privada (prova de posse da chave privada).

Os certificados emitidos pela Entidade de Certificação da GTS:

- Têm um limite de validade (1, 2 ou 3 anos), indicado no seu conteúdo.
- São assinados pela Entidade de Certificação da GTS.
- São distribuídos através de sistemas públicos.
- Podem ser guardados em qualquer tipo de unidades de armazenamento.

Serviços de segurança que requeiram a chave pública do utilizador podem precisar de validar toda a cadeia de confiança da EC GTS (Certificado da Entidade de Certificação da GTS e Certificado da Entidade de Certificação de Raiz da GTS). Estes certificados são públicos e podem ser consultados por qualquer serviço de segurança (<https://pki.globaltrustedsign.com/index.html>).

A emissão deste certificado a ser publicado contém a si inerente a introdução de dois domínios para o site do cliente, utilizando as versões www e não www do URL (por exemplo, "http://www.example.com" e "http://example.com").

O armazenamento das chaves envolvidas em todos os processos de assinatura ou geração de certificados pela Entidade de Certificação da GTS são guardados num Dispositivo Seguro de Hardware (HSM) certificado e que cumpre os requisitos definidos nas normas ETSI.

O perfil do certificado de autenticação de sítios web está de acordo com o conjunto de standards ETSI 319 412 e com as recomendações do CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

#### **10.1.1. Número da Versão**

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

#### **10.1.2. 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.

### 10.1.3. Emissão de Certificados de Autenticação de Sítios Web (SSL Organization Validation)

Componente do Certificado	Valor	Tipo	Comentários
<b>Version</b>	V3	M	
<b>Serial Number</b>	<atribuído pela EC a cada certificado>	M	
<b>Signature</b>	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado. Valor tem que ser igual ao OID no <i>SignatureAlgorithm</i> (abaixo)
<b>Issuer</b>		M	
Country (C)	"PT"		
OrganizationIdentifier	"VATPT-511135610"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Certification Authority 001		
<b>Validity</b>		M	Validade do Certificado
Valid from	<data de emissão>		
Valid to	<data de emissão + (1,2 ou 3 anos)>		Validade máxima de 3 anos.
<b>Subject</b>		M	
Country (C)	<País>		País onde se encontra a entidade
Locality Name (L)	<Localidade>		Localidade onde se encontra filiada a Organização
Organization (O)	<Nome da Organização> (Pessoa Coletiva)		Nome legal da Organização (Pessoa Coletiva)

	<Nome do titular> (Pessoa Singular)		Nome do titular (ou pseudónimo) (pessoa singular)
Common Name (CN)	<Fully Qualified Domain Name do Servidor Web >		
<b>Subject Public Key Info</b>		M	
algorithm	rsaEncryption (OID: 1.2.840.113549.1.1.1)		Algoritmo da chave pública
subjectPublicKey	<Chave Pública>		Chave pública do certificado
<b>Authority Key Identifier</b>		M	
keyIdentifier	160 bit hash		Permite identificar a chave pública correspondente à chave privada do certificado
<b>Subject Key Identifier</b>	160 bit hash	M	Identificador da chave do certificado
<b>Key Usage</b>		M	
Digital Signature	"1" selecionado		
Non Repudiation	"0" selecionado		
Key Encipherment	"1" selecionado		
Data Encipherment	"1" selecionado		
Key Agreement	"0" selecionado		
Key Certificate Signature	"0" selecionado		
CRL Signature	"0" selecionado		
Encipher Only	"0" selecionado		
Decipher Only	"0" selecionado		
<b>Certificate Policies</b>		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.1.2.1.1 Policy Qualifier Id=CPS cPSuri: <a href="https://pki.globaltrustedsign.com/index.html">https://pki.globaltrustedsign.com/index.html</a>		Identificador e localização da Declaração de Práticas de Certificação da EC GTS



[2]	Policy Qualifier Id=0.4.0.194112.1.4		Identifica que o certificado é emitido para autenticação de sítios web (artigo 3 e 45 do Regulamento Europeu Nº 910/2014)
Subject Alternative Name		O	
GeneralName	DNS=<fully qualified domain name do servidor Web>		Máximo 7 Domínios
Basic Constraints		M	
Subject Type	End Entity		Certificado destinado a Entidades Finais
PathLenConstraint	None		
Extended Key Usage		M	
KeyPurposeID	Server Authentication		OID 1.3.6.1.5.5.7.3.1
keyPurposeID	Client Authentication		OID 1.3.6.1.5.5.7.3.2
CRLDistributionPoints		M	
[1]	distributionPoint: <a href="https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl">https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl</a>		Localização da Lista de Revogação de Certificados da EC GTS
[2]	distributionPoint: <a href="https://pki02.globaltrustedsign.com/subca/gts_subca_crl.crl">https://pki02.globaltrustedsign.com/subca/gts_subca_crl.crl</a>		Localização secundária da Lista de Revogação de Certificados da EC GTS
Authority Information Access		M	
accessMethod	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)		Parâmetro usado para identificar o end-point do serviço OCSP
accessLocation	<a href="https://ocsp.globaltrustedsign.com/">https://ocsp.globaltrustedsign.com/</a>		Localização do serviço OCSP
accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parâmetro usado para identificar o certificado da EC GTS e construir a cadeia de confiança.
accessLocation	<a href="https://pki.globaltrustedsign.com/subca/gts_subca.crt">https://pki.globaltrustedsign.com/subca/gts_subca.crt</a>		Localização do certificado da EC GTS
Qualified Certificate Statements		M	

id-etsi-qcs-QcCompliance	<Extensão presente>		A presença do QCStatement afirma que o certificado é um certificado qualificado emitido de acordo com Regulação Europeia (EU) No 910/2014
id-etsi-qcs-QcType	id-etsi-qcs-QcType 3 Certificate for website authentication defined in Regulation (EU) No 910/2014		Certificado para Autenticação de sítios Web como definido na Regulação Europeia (EU) No 910/2014
Id-etsi-qcs-QcPDS	Id-etsi-qcs-QcPDS en: <a href="https://pki.globaltrustedsign.com/index.html">https://pki.globaltrustedsign.com/index.html</a> pt: <a href="https://pki.globaltrustedsign.com/index.html">https://pki.globaltrustedsign.com/index.html</a>		Este QCStatement contém URLs para declarações de divulgação de princípios EC GTS (PDS)
<b>Signature Algorithm</b>	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	m	Algoritmo usado para a criação da assinatura do certificado
<b>Signature Value</b>	<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 PSQ GTS para assinar o certificado. 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], '-', '\_', '.', '\')

#### **10.1.6. OID e sintaxe da Política de Certificados**

A extensão "certificate policies" contém a sequência de um ou mais termos informativos sobre a política, cada um dos quais consiste num identificador da política e qualificadores opcionais.

A sintaxe da sub-extensão "Policy Qualifier" não tem nenhum requisito imposto pelo RFC 3647, no entanto, a EC GTS usa o qualifier cPSuri para indicar o URL das Políticas de Certificados usadas para a emissão de certificados.

A variável opcional Policy Qualified ID (1.3.6.1.5.5.7.2.1) diz respeito ao mecanismo para distribuir mais informação sobre as políticas de certificados.

A variável cPSuri representa um URL onde pode ser encontrada a Política de Certificados de Autenticação de Sítios Web da EC GTS.

#### **10.1.7. Utilização da extensão Policy Constraints**

Não aplicável.