

POLÍTICA DE CERTIFICADOS DE SELOS ELETRÔNICOS

Global Trusted Sign

Referência do Documento | PL02_GTS_V7

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
10.2. Emissão de Certificados para Selo Eletrónico.....	7
10.4. OID do Algoritmo	10
10.5. Restrições nos Nomes	10
10.6. Extensão Policy Constraints	10

1. Referências	Regulamentação Europeia Nº 910/2014 (Art.º8, Secção 4, Anexo I, Anexo II) ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 412-1 PD CENTS 419 241 :2014 RFC 5280 : Internet X.509 PKI - Certificate and CRL Profile, 2008 RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003.
2. Documentos Associados	PC01_GTS - Processo de Emissão dos Certificados para Assinatura Qualificada DP02_GTS - Declaração de Práticas de Certificação da EC GTS DP04_GTS - Declaração de Divulgação de Princípios da EC GTS
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	25-01-2018 Versão 1 09-02-2018 Versão 2 01-03-2018 Versão 3 15-03-2019 Versão 4 18-05-2020 Versão 5 02-06-2020 Versão 6 23-09-2020 Versão 7
5. Classificação do Documento	D Público

6. Registo da Revisão

N.º da Versão	Elaborado	Aprovado	Motivo
7	SegAdm Sandra Mendes y Fernández	Grupo de Gestão Tolentino de Deus Faria Pereira	Adição de perfil para certificado para a faturação eletrónica

7. Introdução

O presente documento tem como objetivo apresentar a Política de Certificados de Selos Eletrônicos 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 é público, e destina-se aos grupos de trabalho da EC GTS e terceiras partes encarregues de auditar a EC GTS.

É recomendado que o leitor tenha conhecimentos sobre os conceitos de criptografia, infraestruturas de chave-pública e assinatura eletrônica.

8. Contexto Geral

O objetivo do presente documento é a definição dos perfis dos Certificados de Selos Eletrônicos Qualificados emitidos pela EC GTS (Entidade de Certificação da Global Trusted Sign), permitindo assim garantir a fiabilidade dos mesmos. 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 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 Selos Eletrônicos”.

Informação do Documento	
Versão do Documento	7.0
Estado do Documento	Aprovado
OID “Identificador de objeto”	1.3.6.1.4.1.50302.1.1.1.2.1.3
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:

a) Selo eletrónico para assinatura

Atributo	Código	Valor
Country	C	<País do titular>
Organization	O	<Nome legal da Organização>
Common Name	CN	<Nome da organização pela qual é conhecida>
OrganizationUnit	OU	<i>RemoteQSCDManagement</i>
Organization Identifier	OrganizationIdentifier	Identificador único da pessoa coletiva, que deve ser diferente do nome da Organização. (2.5.4.97) Formato VAT<código país>-<NIF da entidade coletiva> (Em conformidade com o 5.1.4 da ETSI 319 412-1)

a) Selo eletrónico para Faturação Eletrónica

Atributo	Código	Valor
Country	C	<País do titular>
Organization	O	<Nome legal da Organização>
Common Name	CN	<Nome da organização pela qual é conhecida>
OrganizationUnit	OU	<i>RemoteQSCDManagement</i>
OrganizationUnit	OU	<i>Certificado para aplicação</i>
Organization Identifier	OrganizationIdentifier	Identificador único da pessoa coletiva, que deve ser diferente do nome da Organização. (2.5.4.97) Formato VAT<código país>-<NIF da entidade coletiva> (Em conformidade com o 5.1.4 da ETSI 319 412-1)

9.2. Uso do certificado e par de chaves pelo titular

A pessoa coletiva identificada pelo DN (*Distinguished Name*) é o titular do Certificado Selos Eletrónicos (ver **9.1.** Atribuição de nomes). O certificado emitido segundo esta política cumpre termos do definido na Legislação Portuguesa aplicável para o efeito.

10. Perfis de Certificado

10.1. Perfil de Certificado

O par chave pública – chave privada está associado a um titular cujo principal uso é a 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 de 1,2 ou 3 ano, 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>).

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 Assinatura Digital Qualificada está de acordo com o conjunto de *standards* ETSI 319 412.

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.

10.2. Emissão de Certificados para Selo Eletrónico

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	
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	"Global Trusted Sign Certification Authority 03"		
Validity			Validade do Certificado
Valid from	<data de emissão>		
Valid to	<data de emissão + 1, 2 ou 3 anos>		Validade máxima de 1, 2 ou 3 anos
Subject		M	
Country (C)	<País>		País de nacionalidade do titular do certificado
OrganizationIdentifier	<Identificador único da pessoa coletiva> (opcional)	M	Identificador único da pessoa coletiva, que deve ser diferente do nome da Organização. (2.5.4.97) Formato VAT<código país>-<NIF da entidade coletiva> (Em conformidade com o 5.1.4 da ETSI 319 412-1)
Organization (O)	<nome da organização>		Localidade onde se encontra filiada a Organização
Common Name (CN)	<Nome da organização pela qual é conhecida>		Nome da organização pela qual é conhecida
OrganizationUnit (OU)	<i>RemoteQSCDManagement</i>		Identificador obrigatório definido no Despacho 155/2017 do GNS
OrganizationUnit (OU)	<i>Certificado para aplicação</i>	O	Específico para a faturação eletrónica
Subject Alternative Name	<Email do titular>		
Subject Public Key Info		M	

Componente do Certificado	Valor	Tipo	Comentários
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	"0" 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		
Extended Key Usage	Email Protection (1.3.6.1.5.5.7.3.4)		
Certificate Policies		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.1.2.1.3 Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identificador e localização da Declaração de Práticas de Certificação da EC GTS
Basic Constraints		M	
Subject Type	End Entity		Certificado destinado a Entidades Finais
PathLenConstraint	None		
CRLDistributionPoints		M	

Componente do Certificado	Valor	Tipo	Comentários
[1]	distributionPoint: https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl		Localização da Lista de Revogação de Certificados da EC GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/subca/gts_subca_crl.crl		Localização secundária da Lista de Revogação de Certificados 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-QcSSCD	<Extensão presente>		Este parâmetro significa que a chave privada associada ao certificado esta guardada num QSCD (Qualified Signature/Seal Creation Device) de acordo com o regulamento EU 910/2014
id-etsi-qcs-QcType	id-etsi-qct-QcType 2 (id-etsi-qct-eseal) Certificate for electronic seals as defined in Regulation (EU) No 910/2014		Certificado para Selo Eletrónico como definido na Regulação Europeia (EU) No 910/2014
id-etsi-qcs-QcPDS	Id-etsi-qcs-QcPDS en: https://pki.globaltrustedsign.com/index.html pt: https://pki.globaltrustedsign.com/index.html		Este QCStatement contém URLs para declarações de divulgação de princípios EC GTS (PDS)
Authority Information Access		M	
[1] accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)		Serviço de validação dos certificados
[1] accessLocation	http://ocsp.globaltrustedsign.com/		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	https://pki.globaltrustedsign.com/subca/gts_subca.crt		Localização do certificado da EC 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

10.4. OID do Algoritmo

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

10.5. Restrições nos Nomes

De modo a garantir a total interoperabilidade entre as aplicações que façam uso de certificados digitais, aconselha-se que apenas sejam utilizados caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ` `; ` _`; ` -`; ` .') nas entradas do diretório X.500.

10.6. Extensão Policy Constraints

Não aplicável.