POLÍTICA DE CERTIFICADOS DE SELOS ELETRÓNICOS AVANÇADOS

Global Trusted Sign

Referência do Documento | PL17_GTS_V3

ÍNDICE

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	PC21_GTS - Processo de Emissão dos Certificados Avançados PC22_GTS - Processo de Revogação dos Certificados Avançados
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	03-04-2019 | Versão 1 10-03-2020 | Versão 2 18-09-2020 | Versão 3
5. Classificação do Documento	D | Público

6. Registo da Revisão

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	18-09-2020	18-09-2020	
3	**AdmSeg**	**Grupo de Gestão**	Atualização de registo de colaboradores 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: 18-09-2020 08:58:59	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 18-09-2020 09:00:59	

7. Introdução

O presente documento tem como objetivo apresentar a Política de Certificados de Selos Eletrónicos Avançados da Entidade Certificadora da Global Trusted Sign, enquanto prestadora de serviços de confiança 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 eletrónica.

8. Contexto Geral

O objetivo do presente documento é a definição dos perfis dos Certificados de Selos Eletrónicos Avançados emitidos pela EC NQ GTS (Entidade de Certificação Avançada 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 Eletrónicos".

Informação do Documento	
Versão do Documento	3.0
Estado do Documento	Aprovado
OID "Identificador de objeto"	1.3.6.1.4.1.50302.1.1.2.7.1.0
Data de Emissão	18 de setembro de 2020
Validade	18 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	<País do titular>
Organization	O	<Nome legal da Organização>
Common Name	CN	<Nome da organização pela qual é conhecida>
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 chaves públicas – 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 Avançada da GTS:

- Têm um limite de validade de 1, 2 ou 3 anos, indicado no seu conteúdo.
- São assinados pela Entidade de Certificação Avançada 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 de Raiz da GTS e o Certificado da Entidade de Certificação Avançada). 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 ficam na posse do titular do certificado, uma vez que este certificado é descarregado pelo próprio, cumprindo desta forma os requisitos definidos nas normas ETSI.

O perfil do certificado de Assinatura Digital Avançada 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.

10.1.3. Emissão de Certificados para Selo Eletrónico Avançado

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 NQ Certification Authority 02"		
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>		Nome da organização
Common Name (CN)	<Nome da organização pela qual é conhecida>		Nome da organização pela qual é conhecida
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	

Componente do Certificado	Valor	Tipo	Comentários
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		
Certificate Policies		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.2.7.1.0 Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identificador e localização da Declaração de Práticas de Certificação da EC NQ GTS
Basic Constraints		M	
Subject Type	End Entity		Certificado destinado a Entidades Finais
PathLenConstraint	None		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/subca_nq/gts_subcanq02_crl.crl		Localização da Lista de Revogação de Certificados da EC NQ GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/subca_nq/gts_subcanq02_crl.crl		Localização secundária da Lista de Revogação de Certificados da EC NQ GTS

Componente do Certificado	Valor	Tipo	Comentários
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-nq.globaltrustedsign.com/		Localização do serviço OCSP
[2] accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parâmetro usado para identificar o certificado da EC NQ GTS e construir a cadeia de confiança.
[2] accessLocation	https://pki.globaltrustedsign.com/subca_nq/gts_subcanq02.crt		Localização do certificado da EC NQ 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 NQCA>	M	Assinatura do certificado

10.1.4. 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).

10.1.5. 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.

10.1.6. Extensão *Policy Constraints*

Não aplicável.