POLÍTICA DE CERTIFICADOS PARA ASSINATURAS AVANÇADAS

Global Trusted Sign

Referência do Documento | PL16_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 08:59:00	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 Assinatura Avançada 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 Assinatura Digital Avançada para pessoa Singular e pessoa Coletiva, básica ou profissional 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 de Assinatura Avançada".

Informação do Documento	
Versão do Documento	3.0
Estado do Documento	Aprovado
OID "Identificador de objeto"	1.3.6.1.4.1.50302.1.1.2.6.1.0
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:

- Pessoa Singular (*Natural Person*)

Atributo	Código	Valor
Country	C	<País do titular>
Organization	O	<Nome legal da Pessoa Singular> OU <Nome do Pseudónimo> (Pseudónimo)
Common Name	CN	<Nome do titular do certificado>
Surname	SN	<Nome de família do titular>
Given Name	givenName	<Parte do nome do titular que não é o nome de família nem os nomes intermédios>
Serial Number	serialNumber	Identificador único da pessoa singular. Formato IDC<código país>-< Identificação Civil da pessoa singular>

- Pessoa Coletiva (*Legal Person*)

Atributo	Código	Valor
Country	C	<País do titular>
Organization	O	<Nome legal da Organização>
Common Name	CN	<Nome do titular do certificado>
Surname	SN	<Nome de família do titular>
Given Name	givenName	<Parte do nome do titular que não é o nome de família nem os nomes intermédios>
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)
Serial Number	serialNumber	Identificador único da pessoa singular. Formato IDC<código país>-< Identificação Civil da pessoa singular que representa a entidade coletiva>

- Pessoa Singular Professional (*Natural Person Professional*)

Atributo	Código	Valor
Country	C	<País do titular>
Organization	O	<Nome legal da Pessoa Singular> OU <Nome do Pseudónimo> (Pseudónimo)
Organization Unit	OU	<Descrição da ordem profissional>
Organization Unit	OU	<Código da ordem profissional>-<Número da cédula profissional>
Organization Unit	OU	<Descrição da profissão desempenhada>
Organization Unit	OU	<Nome da organização onde exerce>
Common Name	CN	<Nome do titular do certificado>
Surname	SN	<Nome de família do titular>
Given Name	givenName	<Parte do nome do titular que não é o nome de família nem os nomes intermédios>
Serial Number	serialNumber	Identificador único da pessoa singular. Formato IDC<código país>-< Identificação Civil da pessoa singular>

- Pessoa Coletiva Profissional (Legal Person Professional)

Atributo	Código	Valor
Country	C	<País do titular>
Organization	O	<Nome legal da Organização>
Organization Unit	OU	<Descrição da ordem profissional>
Organization Unit	OU	<Código da ordem profissional>-<Número da cédula profissional>
Organization Unit	OU	<Descrição do cargo desempenhado>
Organization Unit	OU	<Descrição da área/departamento>
Common Name	CN	<Nome do titular do certificado>
Surname	SN	<Nome de família do titular>
Given Name	givenName	<Parte do nome do titular que não é o nome de família nem os nomes intermédios>
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)
Serial Number	serialNumber	Identificador único da pessoa singular. Formato IDC<código país>-< Identificação Civil da pessoa singular que representa a entidade coletiva>

9.2. Uso do certificado e par de chaves pelo titular

A pessoa singular ou coletiva identificada pelo DN (*Distinguished Name*) é o titular do Certificado de Assinatura Digital Avançada (ver 9.1. Atribuição de nomes). O certificado emitido segundo esta política cumpre termos do definido na Legislação Portuguesa aplicável para o efeito, sendo utilizado em qualquer aplicação para quaisquer efeitos de assinatura digital avançada.

10. Perfis de Certificado

10.1. Perfil de Certificado

O par chave pública – chave privada está associado a um titular (pessoa singular ou coletiva) cujo principal uso é a assinatura digital, encriptação e controle de acessos, incluindo a prova de identidade do seu detentor. 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.

10.2. Número da Versão

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

10.3. 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.

10.4. Emissão de Certificados Avançados de Assinatura para Pessoa Coletiva (Legal Person)

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<Atribuído pela Entidade de Certificação Avançada da GTS 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			
Country (C)	<País>	M	País de nacionalidade do titular do certificado
Organization (O)	<Nome legal da Organização>	M	
Common Name (CN)	<Nome comum da pessoa coletiva>		Identificador único do titular do certificado
Surname (SN)	<Nome de família do titular>	M	
Givenname (G)	<Parte do nome do titular que não é o nome de família nem os nomes intermédios>	M	
Serial Number (serialNumber)	<identificador único do certificado>	M	Identificador único da pessoa singular. Formato IDC<código país>-< Identificação Civil da pessoa singular que representa a entidade coletiva> (Em conformidade com o 5.1.3. da ETSI319 412-1)

Componente do Certificado	Valor	Tipo	Comentários
OrganizationIdentifier	<Identificador único da pessoa coletiva>	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)
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	"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: 1.3.6.1.4.1.50302.1.1.2.6.1.0 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	

Componente do Certificado	Valor	Tipo	Comentários
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
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

10.5. Emissão de Certificados Avançados de Assinatura para Pessoa Singular (Natural Person)

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<Atribuído pela EC Avançada 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"		
Organization (O)	"ACIN iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	"Global Trusted Sign NQ Certification Authority 02"		
Validity		M	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
Common Name (CN)	<nome do titular do certificado>		
Surname (SN)	<nomes de família do titular do certificado>	M*	
Given Name (givenName)	<nomes próprios do titular do certificado>	M*	
Organization (O)	<Nome legal da Pessoa Singular> OU <Nome do Pseudónimo> (Pseudónimo)	M*	Nome da legal da Pessoa Singular ou, em alternativa, o seu Pseudónimo, seguido do termo '(Pseudónimo)', indicativo dos casos em que é feito o uso de um Pseudónimo
Serial Number (serialNumber)	<identificador único do certificado>	M	Identificador único da pessoa singular natural. Formato IDC<código país>-< Identificação Civil da pessoa singular> (Em conformidade com o 5.1.3. da ETSI319 412-1)

Componente do Certificado	Valor	Tipo	Comentários
OrganizationIdentifier	<Identificador único da pessoa singular com pseudónimo>	O*	Identificador único da pessoa coletiva, que deve ser diferente do nome da Organização. (2.5.4.97) Formato VAT<código país>-<NIF da pessoa singular com pseudónimo>
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	"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: 1.3.6.1.4.1.50302.1.1.2.6.1.0 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	

Componente do Certificado	Valor	Tipo	Comentários
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
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
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_nq/gts_subcanq02.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 NQCA>	M	Assinatura do certificado

10.6. Emissão de Certificados Avançados de Assinatura para Pessoa Coletiva Professional (Legal Person Professional)

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<Atribuído pela Entidade de Certificação da GTS a cada certificado>	M	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	
Issuer		M	

Componente do Certificado	Valor	Tipo	Comentários
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			
Country (C)	<País>	M	País de nacionalidade do titular do certificado
Organization (O)	<Nome legal da Organização>	M	
OrganizationUnit (OU)	<Descrição da ordem profissional>	O	
OrganizationUnit (OU)	<Código da ordem profissional>-<Número da cédula profissional>	O	
OrganizationUnit (OU)	<Descrição do cargo desempenhado>	M	
OrganizationUnit (OU)	<Descrição da área/departamento>	O	
Common Name (CN)	<Nome comum da pessoa coletiva>		Identificador único do titular do certificado
Surname (SN)	<Nome de família do titular>	M	
Givenname (G)	<Parte do nome do titular que não é o nome de família nem os nomes intermédios>	M	
Serial Number (serialNumber)	<identificador único do certificado>	M	Identificador único da pessoa singular. Formato IDC<código país>-< Identificação Civil da pessoa singular que representa a entidade coletiva> (Em conformidade com o 5.1.3. da ETSI319 412-1)
OrganizationIdentifier	<Identificador único da pessoa coletiva>	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)

Componente do Certificado	Valor	Tipo	Comentários
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	"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: 1.3.6.1.4.1.50302.1.1.2.6.1.0 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_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
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
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_nq/gts_subcanq02.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 NQCA>	M	Assinatura do certificado

10.7. Emissão de Certificados Avançados de Assinatura para Pessoa Singular Professional (Natural Person Professional)

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"		
Organization (O)	"ACIN iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		

Componente do Certificado	Valor	Tipo	Comentários
Common Name (CN)	"Global Trusted Sign NQ Certification Authority 02"		
Validity		M	Validade do Certificado
Valid from	<data de emissão>		
Valid to	<data de emissão + 1 ano>		Validade máxima de 1 ano
Subject		M	
Country (C)	<País>		País de nacionalidade do titular do certificado
OrganizationUnit (OU)	<Descrição da ordem profissional>	O	
OrganizationUnit (OU)	<Código da ordem profissional>-<Número da cédula profissional>	O	
OrganizationUnit (OU)	<Descrição da profissão desempenhada>	M	
OrganizationUnit (OU)	<Nome da organização onde exerce>	O	
Common Name (CN)	<nome do titular do certificado>		
Surname (SN)	<nomes de família do titular do certificado>	M*	
Given Name (givenName)	<nomes próprios do titular do certificado>	M*	
Organization (O)	<Nome legal da Pessoa Singular> OU <Nome do Pseudónimo> (Pseudónimo)	M*	Nome da legal da Pessoa Singular ou, em alternativa, o seu Pseudónimo, seguido do termo '(Pseudónimo)', indicativo dos casos em que é feito o uso de um Pseudónimo
Serial Number (serialNumber)	<identificador único do certificado>	M	Identificador único da pessoa singular natural. Formato IDC<código país>-< Identificação Civil da pessoa singular> (Em conformidade com o 5.1.3. da ETSI319 412-1)
OrganizationIdentifier	<Identificador único da pessoa singular com pseudónimo>	O*	Identificador único da pessoa coletiva, que deve ser diferente do nome da Organização. (2.5.4.97) Formato VAT<código país>-<NIF da pessoa singular com pseudónimo>
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		
Certificate Policies		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.2.6.1.0 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	
[1]	distributionPoint: https://pki.globaltrustedsign.com/subca_nq/gts_subcanq02_crl.crl		Localização da Lista de Revogação de Certificados da EC NQ GTS

Componente do Certificado	Valor	Tipo	Comentários
[2]	distributionPoint: https://pki02.globaltrustedsign.com/subca_nq/gts_subcanq02_crl.crl		Localização secundária da Lista de Revogação de Certificados da EC NQ GTS
Qualified Certificate Statements		M	
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
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_nq/gts_subcanq02.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 NQCA>	M	Assinatura do certificado

M – Mandatório, O – Opcional
* - (Given Name (givenName) e Surname (surname)) ou (Organization (O) com Pseudónimo) é Mandatório.

10.8. 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).

10.9. 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.

10.10. Extensão Policy Constraints

Não aplicável.