POLÍTICA DE CERTIFICADOS DA ROOT CA DA GTS

Global Trusted Sign

Referência do Documento | PL11_GTS_V7

ÍNDICE

1. Referências	Regulamentação Europeia Nº 910/2014 ETSI EN 319 411-1 | 6.5.1 ETSI EN 319 411-2 | 6.5.1 BRG CA/Browser Forum | 6.1.7; 7.1
2. Documentos Associados	DP01_GTS - Declaração de Práticas de Certificação da Root CA GTS DP05_GTS - Declaração de Divulgação de Princípios da ROOT CA GTS
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	31-07-2017 | Versão 1 15-01-2018 | Versão 2 31-01-2019 | Versão 3 13-12-2019 | Versão 4 06-03-2020 | Versão 5 24-06-2020 | Versão 6 17-09-2020 | Versão 7
5. Classificação do Documento	D | Público

6. Registo da Revisão

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	17/09/2020	**17/09/2020**	
	AdmSeg	**Grupo de Gestão**	
	Sandra Mendes y Fernández	**Tolentino de Deus Faria Pereira**	
7	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 17-09-2020 13:44:22	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 17-09-2020 15:48:18	Atualização de registo de colaboradores do Grupo de Confiança da GTS

7. Introdução

7.1. Objetivo

O objetivo deste documento é apresentar a Política de Certificados da Entidade Certificadora Raiz da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014 (adiante designada por ROOT CA GTS).

7.2. Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da ROOT CA GTS;
- Terceiras partes, encarregues de auditar a ROOT CA GTS;
- Todo o público, em geral.

7.3. Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave-pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focados antes de proceder com a leitura do documento.

8. Contexto Geral

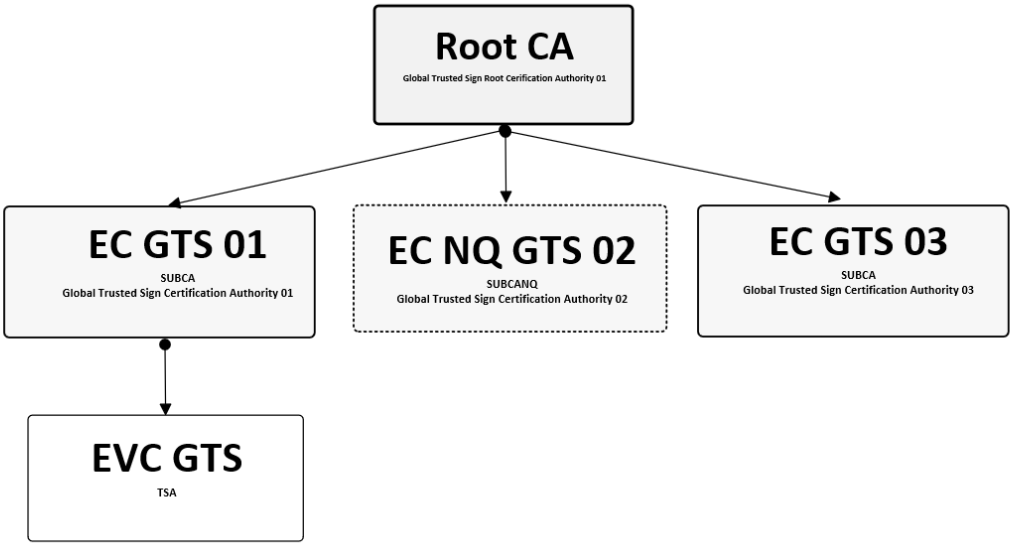
O objetivo do presente documento é a definição do Política de Certificados da ROOT CA GTS. Não se pretende nomear as regras legais ou obrigações, mas antes informar, pelo que se pretende que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Os certificados emitidos pela ROOT CA GTS contêm uma referência à Declaração de Práticas de Certificação da ROOT CA GTS (DPC) 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 ROOT CA GTS.

As Entidades de Certificações (EC01 e 03) da GTS é assinada pela Root CA GTS, assim como a Entidade de Certificação Não Qualificada (EC NQ02). A entidade de Validação Cronológica (EVC) da GTS é assinada pela Entidade de Certificação EC01, inserindo-se assim numa hierarquia de confiança, representada na seguinte figura:



Legenda:

1 – **Root CA GTS** - Entidade Certificadora Raiz da GTS
2 – **EC GTS 01** – Entidade Certificadora da GTS
3 – **EC NQ GTS 02** – Entidade Certificadora Não Qualificada da GTS
4 – **EVC GTS** – Entidade Certificadora de Validação Cronológica da GTS
5 – **EC GTS 03** – Entidade Certificadora da GTS

8.2. Designação e Identificação do Documento

Este documento é a Política de Certificados da ROOT CA GTS (adiante designada por PC). A 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	7.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.2.1.1.0
Data de Emissão	17 de setembro de 2020
Validade	17 de setembro de 2021
Localização	https://pki.globaltrustedsign.com/index.html

8.3. Contacto

A gestão da política de certificados da ROOT CA GTS é da responsabilidade do grupo de Administração de Segurança da mesma.

Nome	Grupo de Administração de Segurança da ROOT CA GTS
Morada	ACIN iCloud Solutions Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira Portugal
Correio Eletrónico	info@globaltrustedsign.com
Página Internet	https://www.globaltrustedsign.com
Telefone	707 451 451

9. Identificação e Autenticação

9.1. Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela DPC da ROOT CA GTS.

9.1.1. Tipos de nomes

O certificado da ROOT CA GTS é identificado por um nome único (DN – Distinguished Name) de acordo com o standard X.500.

Atributo	Código	Valor
Common Name	CN	CN = Global Trusted Sign Root Certification Authority 01
Organization Unit	OU	OU = Global Trusted Sign
Organization	O	O = ACIN-iCloud Solutions, Lda
Country	C	C = PT

9.2. Uso do certificado e par de chaves pelo titular

A ROOT CA GTS é a titular do certificado auto-assinado da Global Trusted Sign Root Certification Authority 01. Este certificado é utilizado para assinar as entidades certificadoras subordinadas que pertencem à hierarquia da ROOT CA GTS, bem com a própria Lista de Revogação de Certificados, nos termos definidos na Declaração de Práticas de Certificação.

10. Perfis de Certificados

O perfil do certificado da ROOT CA GTS está de acordo com o conjunto de standards:

- Regulamento (UE) N. o 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers, e os standards relacionados com os serviços qualificados de confiança.
- Recomendação ITU.T X.5099
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of PubliclyTrusted Certificates.

10.1.1. Perfil de Certificado Qualificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. Essa confiança é dada através do uso de certificados digitais X.509 v3, que são a estrutura de dados que faz a ligação entre a chave pública e o seu titular. Esta ligação é garantida através da assinatura digital de cada certificado pela Entidade Certificadora (EC) de confiança.

O armazenamento das chaves envolvidas em todos os processos de assinatura ou geração de certificados são guardados num Dispositivo Seguro de Hardware (HSM) certificado e que cumpre os requisitos definidos na legislação nacional e europeia.

10.1.2. Perfil de Certificado Não Qualificado

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 Não Qualificada da GTS:

- Têm um limite de validade de 1, 2 ou 3 anos, indicado no seu conteúdo.
- São assinados pela Entidade de Certificação Não Qualificada 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 Não Qualificada). 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 Não Qualificada está de acordo com o conjunto de standards ETSI 319 412.

10.1.3. Número da Versão

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

10.1.4. 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.

10.1.5. 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.

11. Perfil de Certificado Auta assinado

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<atribuído pela EC a cada certificado>	M	Identificador único do certificado
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Root Certification Authority 01		
Validity		M	Validade do Certificado
Valid from	<data de emissão>		01/07/2017
Valid to	<data de emissão + 20 anos>		Validade máxima de 20 anos
Subject		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	<Fully Qualified Domain Name da Entidade Certificadora>		
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	
keyID	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	"0" selecionado		
Key Encipherment	"0" selecionado		
Data Encipherment	"0" selecionado		
Key Agreement	"0" selecionado		
Key Certificate Signature	"1" selecionado		
CRL Signature	"1" selecionado		
Off-line CRL Signing	"1" selecionado		
Encipher Only	"0" selecionado		
Decipher Only	"0" selecionado		
Basic Constraints		M	
Subject Type	CA		Certificado destinado a Entidades Certificadoras
PathLenConstraint	None		
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 ROOT CA>	M	Assinatura do certificado

12. Perfil de Certificado para Entidade Certificadora Qualificada 01

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<atribuído pela EC a cada certificado>	M	Identificador único do certificado
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Root Certification Authority 01		
Validity		M	Validade do Certificado
Valid from	<data de emissão>		11/08/2017
Valid to	<data de emissão + 6 anos>		Validade máxima de 6 anos
Subject		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 01"		<CA Fully Qualified Domain Name >
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	
keyID	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	"0" selecionado		
Key Encipherment	"0" selecionado		
Data Encipherment	"0" selecionado		
Key Agreement	"0" selecionado		
Key Certificate Signature	"1" selecionado		
CRL Signature	"1" selecionado		
Off-line CRL Signature	"1" selecionado		
Encipher Only	"0" selecionado		
Decipher Only	"0" selecionado		
Certificate Policies		M	
policyIdentifier	1.3.6.1.4.1.50302.1.1.1.2.1.0		Identificador e localização da Declaração de Práticas de Certificação da EC GTS
policyQualifiers	Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Localização da Declaração de Práticas de Certificação da EC GTS

Basic Constraints		M	
Subject Type	CA		Certificado destinado a Entidades Certificadoras
PathLenConstraint	None		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_root_crl.crl		Localização da Lista de Revogação de Certificados da ROOT CA GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_root_crl.crl		Localização secundária da Lista de Revogação de Certificados da ROOT CA GTS
Authority Information Access		M	
accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parâmetro usado para identificar o certificado da CA ROOT GTS e construir a cadeia de confiança.
accessLocation	https://pki.globaltrustedsign.com/root/gts_root.crt		Localização do Certificado da CA ROOT 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 GTS>	M	Assinatura do certificado

13. Perfil de Certificado para Entidades de Validação Cronológica (TSA)

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<Atribuído pela EC a cada certificado>	M	Identificador único do certificado
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado
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 01"		
Validity		M	Validade do Certificado
Valid from	<data de emissão>		02/03/2018
Valid to	<data de emissão + 5 anos>		Validade máxima de 5 anos
Subject		M	
Country (C)	"PT"		
Organization (O)	"ACIN iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	"Global Trusted Sign Timestamping Authority 001"		<TSA Fully Qualified Domain Name>

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	
keyID	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		
Extended Key Usage			
Client Authentication	1.3.6.1.5.5.7.3.8	M	
Certificate Policies		M	
policyIdentifier	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
policyQualifiers	policy-identifier: 0.4.0.2023.1.1 cPSuri: https://pki.globaltrustedsign.com/index.html		best-practices-ts-policy

			Identificador e localização na política de Certificados de Selos Temporais
Basic Constraints			
CA	FALSE		Certificado destinado a Entidades Certificadoras
PathLenConstraint	0		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl		Localização da Lista de Revogação de Certificados da SUBCA GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/subca/gts_subca__crl.crl		Localização secundária da Lista de Revogação de Certificados da SUBCA GTS
Authority Information Access		M	
accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parâmetro usado para identificar o certificado da SUBCA GTS e construir a cadeia de confiança.
accessLocation	https://pki.globaltrustedsign.com/subca/gts_subca.crt		Localização do Certificado 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 ROOT CA GTS>	M	Assinatura do certificado

14. Perfil de Certificado para Entidade Certificadora Subordinada Não Qualificada

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<Atribuído pela Entidade de Certificação a cada certificado>	M	Identificador único do certificado.
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado.
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Root Certification Authority 01		
Validity		M	Validade do Certificado
Valid from	<data de emissão>		23/03/2019
Valid to	<data de emissão + 6 anos>		Validade máxima de 6 anos.
Subject			
Country (C)	<País>	M	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 NQ Certification Authority 02"		<Non-Qualified CA Fully Qualified Domain Name >
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

Componente do Certificado	Valor	Tipo	Comentários
Subject Key Identifier	160 bit hash	M	Identificador da chave do certificado
Key Usage		M	
Digital Signature	"0" selecionado		
Non Repudiation	"0" selecionado		
Key Encipherment	"0" selecionado		
Data Encipherment	"0" selecionado		
Key Agreement	"0" selecionado		
Key Certificate Signature	"1" selecionado		
CRL Signature	"1" selecionado		
Off-line CRL Signature	"1" selecionado		
Encipher Only	"0" selecionado		
Decipher Only	"0" selecionado		
Certificate Policies		M	
policyIdentifier	policyIdentifier: 1.3.6.1.4.1.50302.1.1.1.1.1.0		Identificador e localização da Declaração de Práticas de Certificação da EC GTS
policyQualifiers	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	CA		Certificado destinado a Entidades Certificadoras
PathLenConstraint	None		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_root_crl.crl		Localização da Lista de Revogação de Certificados da ROOT CA GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_root_crl.crl		Localização secundária da Lista de Revogação de Certificados da ROOT CA GTS

Componente do Certificado	Valor	Tipo	Comentários
Authority Information Access		M	
accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parâmetro usado para identificar o certificado da ROOT CA GTS e construir a cadeia de confiança.
accessLocation	https://pki.globaltrustedsign.com/root/gts_root.crl		Localização do certificado da ROOT CA 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

15. Perfil de Certificado para Entidade Certificadora Qualificada 03

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<atribuído pela EC a cada certificado>	M	Identificador único do certificado
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	"Global Trusted Sign Root Certification Authority 01"		
Validity		M	Validade do Certificado
Valid from	<data de emissão>		11/05/2020
Valid to	<data de emissão + 6 anos>		Validade máxima de 6 anos
Subject		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 03"		< CA Fully Qualified Domain >
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	
keyID	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	"0" selecionado		
Key Encipherment	"0" selecionado		
Data Encipherment	"0" selecionado		
Key Agreement	"0" selecionado		
Key Certificate Signature	"1" selecionado		
CRL Signature	"1" selecionado		
Off-line CRL Signature	"1" selecionado		
Encipher Only	"0" selecionado		
Decipher Only	"0" selecionado		
Certificate Policies		M	
policyIdentifier	1.3.6.1.4.1.50302.1.1.1.2.1.0		Identificador e localização da Declaração de Práticas de Certificação da EC GTS
policyQualifiers	Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Localização da Declaração de Práticas de Certificação da EC GTS

Basic Constraints		M	
Subject Type	CA		Certificado destinado a Entidades Certificadoras
PathLenConstraint	None		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/root/gts_root_crl.crl		Localização da Lista de Revogação de Certificados da ROOT CA GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/root/gts_root_crl.crl		Localização secundária da Lista de Revogação de Certificados da ROOT CA GTS
Authority Information Access		M	
accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parâmetro usado para identificar o certificado da CA ROOT GTS e construir a cadeia de confiança.
accessLocation	https://pki.globaltrustedsign.com/root/gts_root.crt		Localização do Certificado da CA ROOT 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 GTS>	M	Assinatura do certificado

16. 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).

17. Extensão Policy Constraints

Não aplicável.