POLÍTICA DE CERTIFICADOS DE SELOS ELETRÓNICOS

Global Trusted Sign

Referência do Documento | PL02_GTS_V8
Classificação do Documento: Público
Data: 06 de maio de 2021

Índice

1. Introdução

Objetivo

O objetivo deste documento é apresentar a Política de Certificados de Selos Eletrónicos da Entidade da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014 adiante designada por EC GTS.

Público Alvo

Este documento deve ser lido por:

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

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. 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.

1.1. Contexto Geral

O presente documento tem como objetivo apresentar a Política de Certificados de Selos Eletrónicos da Entidade Certificadora da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014 (adiante designada por EC GTS). 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. Os certificados emitidos pela EC GTS contêm uma referência à Declaração de Práticas de Certificação da EC GTS, sendo a mesma complementada pela presente Política de Certificação.

O respetivo documento é elaborado tendo como referência a Declaração de Práticas da Entidade de Certificação, DP02_GTS.

1.2. Designação e Identificação do Documento

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

Informação do Documento	
Versão do Documento	8.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.1.2.1.3
Data de Emissão	06 de maio de 2021
Validade	06 de maio de 2022
Localização	https://pki.globaltrustedsign.com/index.html

1.2.1. Registo de revisão

N.º da Versão	Elaborado	Aprovado	Motivo
	06-05-2021	06-05-2021	
8	**AdmSeg**	**Grupo de Gestão**	Atualização de estrutura do documento, de acordo com o RFC 3647
	Sandra Mendes y Fernández Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 06-05-2021 16:05:36	Tolentino de Deus Faria Pereira Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 06-05-2021 16:20:07	

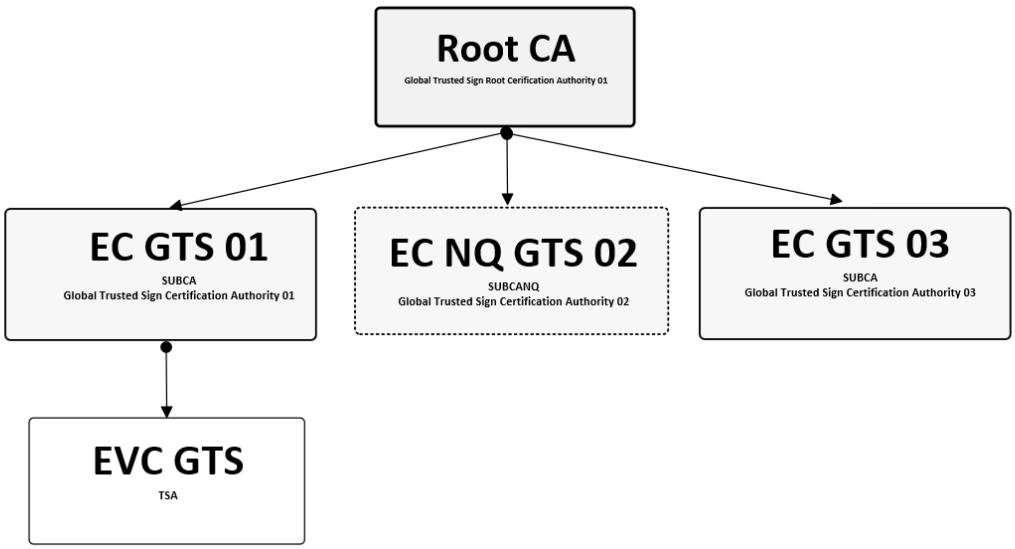
1.2.2. Datas relevantes

Histórico de versões do documento

ID de versão	Data da versão	Motivo de nova versão
Versão 1	25-01-2018	Apresentar a Política de Certificados de Selos Eletrónicos da Entidade Certificadora da Global Trusted Sign
Versão 2	09-02-2018	Atualização de campos dos certificados
Versão 3	01-03-2018	Atualização do formato do Serial Number e Organization Identifier, para cumprimento da ETSI 319 412-1
Versão 4	15-03-2019	Atualização da validade do documento e OCSP
Versão 5	18-05-2020	Novo perfil de certificado para assinar e-mails
Versão 6	02-06-2020	Adição de certificado de SUBCA 03
Versão 7	23-09-2020	Atualização com perfil de certificado para facturação eletrónica
Versão 8	06-05-2021	Atualização de estrutura do documento, de acordo com o RFC 3647

1.3. Participantes na Infraestrutura de Chave Pública

A GTS, enquanto prestador qualificado de serviços de confiança, disponibiliza uma hierarquia de confiança credenciada pelo Gabinete Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), conforme previsto na legislação portuguesa e europeia. É composta por um conjunto de equipamentos, aplicações, recursos humanos e procedimentos indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir assim a adequada gestão do ciclo de vida dos certificados descritos no presente documento. A hierarquia de confiança da GTS é composta pela Entidade Certificadora Raiz da GTS (ROOT CA GTS), as Entidades Certificadoras da GTS (EC GTS01 e EC GTS03), a Entidade Certificadora Não Qualificada da GTS (EC NQ GTS) e a Entidade Certificadora de Selos Temporais da GTS (EVC GTS). Estas entidades certificadoras estão descritas nos pontos 1.3.1.1, 1.3.1.2, 1.3.1.3 e 1.3.1.4 do presente documento e encontram-se ilustradas de seguida:



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**
1 – EC GTS 03 **– Entidade Certificadora da GTS**

1.4. Utilização do Certificado

Os certificados emitidos pelo PKI da GTS são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança, nomeadamente:

- Autenticação;
- Confidencialidade;
- Integridade;
- Privacidade de Dados;
- Não Repúdio;
- Autenticidade.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, mediante a utilização da estrutura de confiança que a PKI da GTS disponibiliza. As Partes Confiantes podem verificar a cadeia de confiança de um certificado emitido pela EC GTS, garantindo assim a autenticidade e identidade do titular. Os certificados qualificados emitidos pela EC GTS estão de acordo com esta DPC e são certificados qualificados em conformidade com os requisitos do regulamento (EU) 910/2014.

1.5. Gestão de Políticas

1.5.1. Entidade Responsável pela Gestão do Documento

A gestão desta declaração de práticas de certificação da EC GTS é da responsabilidade do grupo de Confiança da GTS.

1.5.2. Entidade de Contato

ACIN iCloud Solutions, Lda.
Estrada Regional 104 Nº42-A
9350-203 Ribeira Brava
Madeira – Portugal

Tel: 707 451 451 / + 351 291 957 888

https://www.globaltrustedsign.com
E-mail: info@globaltrustedsign.com

1.6. Definições e Acrónimos

1.6.1. Definições

Definições	
Termo	**Definição**
Assinatura Eletrónica	Dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar
Assinatura Eletrónica Avançada	Assinatura eletrónica que obedeça aos requisitos: a) Esteja associada de modo único ao signatário b) Permita identificar o signatário c) Seja criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo, e d) Esteja ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados
Autenticação	Processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar
Certificado	Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.
Certificado de Assinatura Eletrónica	Atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo
Certificado de Autenticação de Sítio Web	Atestado que torne possível autenticar um sítio web e associe o sítio web à pessoa singular ou coletiva à qual o certificado tenha sido emitido
Certificado de Selo Eletrónico	Atestado eletrónico que associa os dados de validação do selo eletrónico a uma pessoa coletiva e confirma o seu nome
Certificado Qualificado de Assinatura Eletrónica	Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Autenticação de Sítios Web	Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Selo Eletrónico	Certificado de selo eletrónico emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III do Regulamento europeu 910/2014
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves

Definições	
Termo	**Definição**
Credenciação	Ato pelo qual é reconhecido a um prestador de serviços que o solicite e que exerça a atividade de entidade certificadora em conformidade com os requisitos definidos no Regulamento europeu 910/2014
Criador de um Selo	Pessoa coletiva que cria um selo eletrónico
Dados de Identificação Pessoal	Conjunto de dados que permita determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa coletiva
Dados de Validação	Dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico
Dados para a Criação de um Selo Eletrónico	Conjunto único de dados que seja utilizado pelo criador do selo eletrónico para criar um selo eletrónico
Dados para a Criação de uma Assinatura Eletrónica	Conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica
Dispositivo de Criação de Assinaturas Eletrónicas	*Software* ou *hardware* configurados, utilizados para criar assinaturas eletrónicas
Dispositivo de Criação de Selos Eletrónicos	*Software* ou *hardware* configurados, utilizados para criar selos eletrónicos
Dispositivo Qualificado de Criação de Assinaturas Eletrónicas	Dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Dispositivo Qualificado de Criação de Selos Eletrónicos	Dispositivo para a criação de selos eletrónicos que satisfaça *mutatis mutandis* os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Documento Eletrónico	Qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Entidade Certificadora	Entidade ou pessoa singular ou coletiva credenciada como prestador qualificado de serviços de confiança pela entidade supervisora
Entidade de Registo	Entidade que aprova os Nomes Distintos (DN) das entidades subordinadas e, mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo
Entidade Supervisora	Entidade competente para a credenciação e fiscalização das entidades certificadoras
Função Hash	Operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função.
Hash ou Impressão Digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais
HSM	Módulo de segurança criptográfico empregue para armazenar chaves e realizar operações criptográficas de modo seguro
Identificação Eletrónica	O processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva

Definições	
Termo	**Definição**
Infraestrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas
Meio de Identificação Eletrónica	Uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha
OID	Identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica
Organismo de Avaliação da Conformidade	Organismo definido que é acreditado nos termos do regulamento 910/2014 como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados
Organismo Público	Entidade estatal nacional, regional ou local, um organismo de direito público ou uma associação formada por uma ou mais dessas entidades ou por um ou mais organismos de direito público, ou uma entidade privada mandatada por, pelo menos, uma dessas autoridades, organismos ou associações como sendo de interesse público, ao abrigo de tal mandato
Parte Confiante	As partes confiantes ou destinatários são pessoas singulares ou entidades que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação de um selo temporal ao datum, ou seja, confiam na veracidade do selo temporal.
Política de Certificado	Conjunto de regras que indica a aplicabilidade do certificado a uma comunidade específica e/ou classe de aplicação com requisitos de segurança comuns
Prestador de Serviços de Confiança	Pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança
Prestador Qualificado de Serviços de Confiança	Prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora
Produto	*Hardware* ou *software*, ou componentes pertinentes de hardware ou software, que se destinem a ser utilizados para a prestação de serviços de confiança
Selo Eletrónico	Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos

Definições	
Termo	**Definição**
Selo Eletrónico Avançado	Selo eletrónico que obedeça aos requisitos: a) Esteja associado de modo único ao seu criador b) Permita identificar o seu criador c) Seja criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico, e d) Esteja ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dados
Selo Eletrónico Qualificado	Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico
Selo Temporal Qualificado	Selo temporal que satisfaça os requisitos: a) Vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável, b) Basear-se numa fonte horária precisa ligada à Hora Universal Coordenada, e c) Ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente
Selos Temporais	Dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento
Serviço de Confiança	Serviço eletrónico geralmente prestado mediante remuneração, que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços, ou b) Na criação, verificação e validação de certificados para a autenticação de sítios web, ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços
Serviço de Confiança Qualificado	Serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento europeu 910/2014
Serviço de Envio Registado Eletrónico	Serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada

Definições	
Termo	**Definição**
Serviço Qualificado de Envio Registado Eletrónico	Serviço de envio registado eletrónico que satisfaça os requisitos: a) Serem efetuados por um ou mais prestadores qualificados de serviços de confiança b) Garantirem, com um elevado nível de confiança, a identificação do remetente c) Garantir a identificação do destinatário antes da entrega dos dados d) O envio e a receção dos dados serem securizados por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, de modo a tornar impossível a alteração dos dados de forma não detetável e) Qualquer alteração a que devam ser sujeitos para o seu envio ou receção ser claramente indicada ao remetente e ao destinatário dos dados f) A data e a hora do envio e da receção, assim como as eventuais alterações dos dados, serem indicadas por meio de um selo temporal qualificado
Signatário	Pessoa singular que cria uma assinatura eletrónica.
Sistema de Identificação Eletrónica	Sistema de identificação eletrónica ao abrigo do qual sejam produzidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem pessoas coletivas
Titular	Ver Signatário.
Utilizador	Pessoa singular ou coletiva que utiliza a identificação eletrónica ou o serviço de confiança
Validação	Processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico
Validação Cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos

1.6.2. Acrónimos

Acrónimos	
C	*Country*
CN	*Common Name*
DN	Nome Distinto *(Distinguished Name)*
DPC	Declaração de Práticas de Certificação
DR	Decreto Regulamentar
EC	Entidade Certificadora
ER	Entidade de Registo
GNS	Gabinete Nacional de Segurança
GTS	*Global Trusted Sign*
HSM	Modulo Criptográfico em Hardware (*Hardware Secure Module*)
LRC	Lista de Revogação de Certificados
O	*Organization*
OU	*Organization Unit*
OID	Identificador de Objeto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	Infraestrutura de Chave Pública *(Public Key Infrastructure)*
SSL/TLS	*Secure Sockets Layer / Transport Layer Security*

1.6.3. Referências Bibliográficas

- ✓ DP02_GTS - Declaração de Práticas de Certificação da EC GTS
- ✓ PC02_GTS_V5 - Processo de Emissão dos Selos Eletrónicos
- ✓ 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 TS 119 312: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key Certificates;
- ✓ ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, v1.2.0;
- ✓ ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, v1.1.1;
- ✓ ETSI EN 319 401 v2.1.1: General policy requirements for Trust Service Providers;
- ✓ ETSI 319 412 v1.4.2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
- ✓ RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List Profile, 2008;
- ✓ RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;
- ✓ CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.7.3.

2. Responsabilidade de Publicação e Repositório

O repositório das diversas entidades certificadoras pode ser acedido 24x7 em:
https://pki.globaltrustedsign.com/index.html
https://pki02.globaltrustedsign.com/index.html
O repositório será atualizado sempre que haja uma alteração num dos documentos publicados.

3. Identificação e Autenticação

3.1. Atribuição de Nomes

A EC GTS, garante a emissão de certificados contendo um *Distinguished Name* (DN) X.509 a todos os titulares que submetam documentação em formato eletrónico, de acordo com o preconizado no RFC 5280.

3.1.1 Tipos de Nomes

A EC GTS garante que, a atribuição dos nomes, cumpre os requisitos especificados nas políticas de certificados para cada tipo de perfil apresentado. Os vários tipos de certificados podem conter os seguintes campos no DN:

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	*RemoteQSCDManagement*
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)

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	*RemoteQSCDManagement*
OrganizationUnit	OU	*Certificado para aplicação*
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)

3.1.2. Necessidade de Nomes Significativos

A EC GTS assegura que os nomes utilizados nos certificados por ela emitidos identificam de uma forma significativa e clara os seus titulares, assegurando que o DN usado é apropriado para um dado titular e que a componente *Common Name* do DN o representa de forma a ser facilmente identificável pelos interessados.

3.1.3. Anonimato ou Pseudónimo de Titulares

A EC GTS não permitido o anonimato de titulares no processo de emissão de certificados.

3.1.4. Interpretação de Formato de Nomes

As regras utilizadas pela ROOT GTS para interpretar o formato de nomes suguem o estabelecido no *RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* garantindo assim que todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado são codificados numa UTF8String, com exceção dos atributos country e serialnumber que são codificados numa *PrintableString*.

3.1.5. Unicidade de Nomes

Na EC GTS, existem controlos que garantem que o DN e o conteúdo da extensão *Key Usage* são únicos, não ambíguos e referentes apenas a uma entidade, garantindo, assim, a rejeição de emissão de certificados emitidos por esta que, tendo o mesmo nome único, identifiquem entidades distintas

3.2. Validação de Identidade no Registo Inicial

Na EC GTS, existem controlos que garantem que o DN e o conteúdo da extensão *Key Usage* são únicos, não ambíguos e referentes apenas a uma entidade, garantindo, assim, a rejeição de emissão de certificados emitidos por esta que, tendo o mesmo nome único, identifiquem entidades distintas.

Identificação de Pessoa Coletiva

Os documentos obrigatórios apresentados no Formulário devem permitir aos Administradores de Registo validar de forma inequívoca a identidade do Requerente, nomeadamente:

- Da pessoa singular que a representa:
    i. Nomes próprios e Apelido (de acordo com as práticas nacionais para identificação de pessoas)
    ii. Data e local de nascimento

iii. Documento de identificação reconhecido nacionalmente que permita distinguir o titular de outros com o mesmo nome
iv. Documento com valor probatório equivalente à presença física

- Pessoa coletiva:
  i. Nome completo e dados sobre a pessoa coletiva
  ii. Evidência da associação da pessoa singular com a pessoa coletiva que irá aparecer nos atributos do certificado.

3.2.2. Método de Prova de Posse da Chave Privada

Nos casos em que a EC GTS não seja a entidade responsável pela geração do par de chaves criptográficas a atribuir ao utilizador, esta, antes de proceder à sua emissão, assegurará que o utilizador possui a chave privada correspondente à chave pública constante no pedido de certificado. O método de prova será necessariamente tão mais complexo e preciso consoante a importância do tipo de certificado pedido, encontrando-se documentado na Política de Certificado do certificado em causa.

3.2.3. Autenticação de Identidade da Organização e Domínio

O DN emitidos pela EC GTS têm em atenção as marcas registadas, não permitindo a utilização deliberada de nomes registados cuja entidade não possa provar ter direito à marca, podendo-se recusar a emitir o certificado com nomes de marcas registadas se concluir que outra identificação seja mais conveniente.

3.2.4. Autenticação de Identidade do Indivíduo

A verificação da identidade dos subscritores e/ou titulares será efetuada pelo grupo de trabalho de Administradores e pode ser realizada das seguintes formas:

- De forma presencial, sempre com estando presentes neste ato dois administradores de registo (alínea a, do n.º 1, do artigo 24º do Reg.910/2014), ou;
- À distância, utilizando meios de identificação eletrónica, como a videoconferência através de software certificado para o efeito, para os quais tenha sido assegurada, antes da emissão do certificado qualificado, a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva e que cumprem os requisitos estabelecidos no artigo 8.º do regulamento 910/2014 relativamente aos níveis de garantia «substancial» ou «elevado» e o Despacho 154/2017 do GNS, (alínea b, do n.º 1, do artigo 24º do Reg.910/2014), ou
- Por meio de um certificado de assinatura eletrónica qualificada ou de um selo eletrónico qualificado emitido nos termos da alínea anterior (alínea c, d, do n.º 1, do artigo 24º do Reg.910/2014), apenas para cidadãos com cartão de cidadão português.

3.2.5. Informação de Subscritor/Titular não Verificada

Toda a informação fornecida pelo subscritor é verificada.

3.2.6. Validação de Autoridade

Consultar secção 4.

3.2.7. Critérios para a Interoperabilidade

Os certificados emitidos na PKI GTS são emitidos debaixo de uma só hierarquia de confiança.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

4.1. Pedido de Certificado

Um pedido de emissão de certificados à EC GTS inicia-se com o preenchimento de um formulário, desenhado para cada tipo de certificado suportado e com a aceitação dos termos e condições estabelecidos pela EC GTS, devidamente assinados pelo titular de forma manuscrita e que neste caso pressupõe o envio dos documentos originais por CTT para a GTS ou de forma digital, com recurso a assinatura qualificada.

4.1.2. Quem Pode Submeter um Pedido de Certificado

Os pedidos de subscrição de certificados podem ser submetidos pelos seguintes:

- O titular do certificado;
- Um representante do titular do certificado, devidamente autorizado e com poderes para o efeito;
- Uma pessoa coletiva que seja titular do certificado;
- Um representante da GTS.

4.1.3. Processo de Registo e Responsabilidades

Após a receção da documentação dá-se início a um processo de validação da informação e identidade do titular e quando aplicável entidade requerente. Este processo é executado sempre por 2 Administradores de Registo, com o fim de verificar a autenticidade dos dados fornecidos, dependendo do tipo de certificado solicitado. A GTS não utiliza entidades de registo externas para fornecimento do serviço de registo. No caso dos certificados Web/SSL, o formulário deverá ser acompanhado aquando a sua submissão, de um CSR (Certificate Signing Request) que deve conter informação para os campos do certificado, que devem coincidir com os campos inseridos no formulário.

Nota: O pedido de certificado não implica a sua obtenção se o solicitante não cumprir os requisitos estabelecidos nesta DPC. Os pedidos efetuados aceites ou rejeitados serão arquivados e mantidos por um período de 7 anos de acordo com o CAB Fórum secção 5.5.2.

4.2. Processamento do Pedido de Certificado

4.2.2. Desempenho de Funções de Identificação e Autenticação

A GTS, assim que rececione o formulário de pedido de emissão de certificado, bem como a informação necessária à emissão do pedido, procederá à validação de toda a informação disponibilizada a fim de verificar a autenticidade dos dados.

4.2.3. Aprovação ou Rejeição de Pedidos de Certificados

Os pedidos de certificados serão aceites, apenas se, todos os dados do pedido forem autênticos. No caso das informações contantes do processo de avaliação o pedido será rejeitado, sendo o responsável pelo mesmo informado.

4.2.4. Prazo para Emissão do Certificado

A GTS tem 60 minutos após validação da identidade e idoneidade do subscritos e boa cobrança para proceder com a emissão e envio do certificado de autenticação web.

4.3. Emissão de Certificados

4.3.2. Ações da EC durante a Emissão do Certificado

Este processo é executado por dois Administradores de Registo, recorrendo a dupla autenticação com o fim de verificar a autenticidade dos dados fornecidos, dependendo do tipo de certificado solicitado. Os certificados são emitidos por interação da Entidade Certificadora com um módulo criptográfico em hardware (Hardware Secure Module - HSM), tendo por base o tipo de política de certificado aplicável. O certificado de chave pública é armazenado no HSM. No caso dos certificados para autenticação de

sítios web, o certificado emitido inicia a sua vigência no momento da sua emissão e o subscritor do certificado é notificado via correio eletrónico, sendo-lhe enviado, por este canal, o certificado de chave pública.

4.3.3. Notificação ao Subscritor/Titular pela EC Emissora do Certificado

O subscritor do certificado é notificado via correio eletrónico, sendo-lhe enviado, por este canal, o certificado de chave pública.

4.4. Aceitação do Certificado

4.4.2. Conduta que Constitui a Aceitação do Certificado

Antes do envio do certificado de chave pública, o subscritor e titular terão de aceitar as condições de utilização do certificado, considerando-se, assim o mesmo como aceite. Perante o certificado emitido, subscritor deve ser uma entidade consciente dos tópicos seguintes:

- O conhecimento das funcionalidades e conteúdo do certificado;
- O conhecimento dos direitos e responsabilidades.

4.5. Utilização do Certificado e Par de Chaves

4.5.2. Utilização do Certificado e Par de Chaves pelo Subscritor/Titular

Os titulares de certificados utilizam a sua chave privada apenas, e só, para o fim a que estas se destinam (conforme estabelecido no campo do certificado "keyUsage") e sempre com propósitos legais. A utilização do certificado é sempre da responsabilidade do seu titular.

A utilização do certificado apenas é permitida, e caso aplicável para o tipo de certificado em questão:

- A quem estiver designado no campo do certificado Subject;
- Depois de aceitar os termos e condições associados ao tipo de certificado;
- Enquanto o certificado se mantiver válido e não estiver na LRC da EC GTS.

4.5.3. Utilização do Certificado e Chave Pública por Partes Confiantes

As partes confiantes devem usar software em conformidade com os standards X.509 e devem confiar no certificado apenas se este não estiver expirado, suspenso ou revogado. A EC GTS fornece nesta DPC informação sobre os serviços apropriados disponíveis para verificar o estado de validade do certificado, tais como OCSP e CRL.

4.6. Renovação de Certificado

4.6.2. Circunstâncias para a Renovação do Certificado

Para realizar a renovação do seu certificado, e se as funções e informações para as quais o certificado inicial foi emitido se mantiverem, apenas terá de solicitar a renovação do seu certificado com os mesmos dados e efetuar pagamento de renovação seguindo as indicações que lhe serão enviadas pela GTS. Este processo obriga a uma nova geração de um par de chaves, e respetivo certificado.

Se um titular pretender renovar um certificado é desencadeado um procedimento para cada um dos seguintes casos:

Motivo para Renovação	Procedimento de Renovação
O certificado foi revogado	(*i*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com os mesmos campos exceto a chave pública.
O titular pretende prolongar a validade do certificado	(*i*) O antigo certificado é revogado. (*ii*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com os mesmos campos exceto a chave pública.
A informação que deu origem ao certificado sofre alterações	(*i*) O antigo certificado é revogado. (*ii*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com as alterações necessárias incluindo a nova chave pública.

A renovação de certificados utiliza os procedimentos de autenticação e identificação inicial que resultam na geração de novos pares de chaves.

4.6.3. Quem pode Solicitar a Renovação de Certificado

Podem solicitar a renovação de certificados, os Subscritores/Titulares dos mesmos.

4.6.4. Processamento do Pedido de Renovação de Certificado

O processamento do pedido de renovação de certificado, executa-se conforme descrito na secção 5.6.1.

4.6.5. Notificação de Nova Emissão de Renovação de Certificado ao Subscritor/Titular

O subscritor do certificado é notificado via correio eletrónico em tempo razoável após a emissão do certificado, e pode usar qualquer mecanismo confiável para entregar o certificado ao Subscritor.

4.6.6. Conduta que Constitui a Aceitação de Renovação de Certificado

Os certificados renovados são considerados aceites após a sua entrega ou notificação da emissão do certificado ao Subscritor, ou quando exista evidência de que o Subscritor utilizou o certificado.

4.7. Re-Key do Certificado

4.7.2. Circunstâncias para o Re-Key de Certificado

O processo de Re-Key de um certificado não é suportado pela EC GTS.

4.8. Modificação do Certificado

A modificação de certificado é um processo através do qual o certificado é emitido para um Subscritor ou Patrocinador mantendo as mesmas chaves, com alterações apenas na informação do certificado. A modificação de certificados não é suportada pela EC GTS.

4.9. Revogação e Suspensão do Certificado

A revogação de certificados é o mecanismo utilizado, quando por algum motivo, os certificados deixam de ser fiáveis antes do período de finalização originalmente previsto. Na prática, a revogação de certificados é uma ação através da qual, o certificado deixa de estar válido antes do fim do seu período de validade, perdendo, deste modo, a sua operacionalidade. A suspensão de certificados não é suportada pela EC GTS.

4.9.1. Motivos para Revogação

Um certificado pode ser revogado por uma das seguintes razões:

- Cessação de funções;
- Roubo, extravio, destruição ou deterioração do dispositivo de suporte dos certificados;
- Inexatidões nos dados fornecidos;
- Comprometimento ou suspeita de comprometimento das chaves privada do titular;
- Comprometimento ou suspeita de comprometimento da senha de acesso ao certificado;
- Comprometimento ou suspeita de comprometimento das chaves privada da EC GTS;
- Incumprimento por parte da EC GTS ou titular das responsabilidades prevista na DPC;
- Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa;
- Utilização do certificado para atividades abusivas

4.9.2. Quem pode solicitar a revogação

Um pedido de revogação pode ser efetuado de forma legítima por um dos seguintes intervenientes:

- O titular do certificado;
- A Entidade Certificadora ou Entidade Requerente do certificado da entidade subordinada;
- A GTS, no conhecimento de que:
    - Os dados constantes no certificado não correspondem à realidade;
    - O certificado não esteja na posse do seu titular;
- A Entidade Supervisora;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

4.9.3. Procedimento para o Pedido de Revogação

O Pedido de Revogação deve ser efetuado através do serviço disponibilizado para o efeito em https://www.globaltrustedsign.com. A EC GTS irá processar o pedido de revogação em 24 horas seguintes às da receção do pedido. Nesse intervalo de tempo, será verificada a identidade e autenticidade de quem solicitou a revogação do certificado.

4.9.4. Período de Carência do Pedido de Revogação

O período de carência do pedido de revogação é o tempo disponível para o Subscritor tomar as ações necessárias para pedir a revogação de um certificado sobre o qual exista suspeita de comprometimento da chave, utilização de uma chave fraca ou descoberta de informação imprecisa contida no certificado. Nesta situação, o Subscritor deve pedir a revogação no prazo de 24 horas após a sua deteção.

4.9.5. Tempo de Processamento do Pedido de Revogação pela EC

Após a confirmação da identidade e autenticidade do requerente, a TSP GTS tem 60 minutos, para transitar o estado do certificado para revogado.

4.9.6. Requisito de Verificação da Revogação pelas Partes Confiantes

Antes de confiar na informação listada num certificado, a Parte Confiante deve validar a adequação do certificado para a finalidade pretendida e garantir que o certificado é válido. Para verificar o estado do certificado, as Partes Confiantes necessitam consultar as respostas OCSP ou CRL identificadas em cada certificado.

4.9.7. Frequência de Emissão de CRL

Os estados dos certificados emitidos pela ROOT CA da GTS podem ser verificados através da consulta da sua CRL. Esta é emitida sempre que haja uma revogação dos certificados emitidos ou, na ausência de alterações no estado dos certificados, de forma trimestral. A disponibilização nos repositórios é feita num período não superior a 30 minutos, sendo o seu download feito em menos de 10 segundos. De modo a garantir a sua disponibilidade, a CRL é disseminada nos seguintes repositórios:

- https://pki.globaltrustedsign.com/index.html

4.9.8. Latência Máxima para CRL

A GTS dispõe de recursos suficientes para garantir as condições normais de operação, nomeadamente um tempo de resposta menor ou igual a 10 segundos.

4.9.9. Disponibilidade de Verificação de Estado/Revogação Online

A EC GTS dispõe de serviços de validação OCSP do estado dos certificados de forma online. Esse serviço poderá ser acedido em http://ocsp.globaltrustedsign.com

4.9.10. Requisitos de Verificação de Revogação Online

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das LRC ou num servidor de verificação do estado online (via OCSP).

4.9.11. Outras Formas Disponíveis de Anunciar a Revogação

Não estipulado.

4.9.12. Requisitos Especiais Relacionados com o Comprometimento de Chave

Consultar 4.9.1.

4.9.13. Motivos para suspensão

O processo de suspensão de um certificado não é suportado pela EC GTS.

4.10. Serviços de Estado do Certificado

4.10.1. Caraterísticas Operacionais

O estado de certificados emitidos está disponível publicamente utilizando CRL e o serviço OCSP.

4.10.2. Disponibilidade de Serviço

O serviço de estado de certificado está disponível 24 horas por dia, 7 dias por semana. Se um certificado for revogado, este não se mantém na CRL após a sua data de expiração.

4.11. Fim de Subscrição

O fim da subscrição de um certificado ocorre quando o prazo de validade é expirado ou o certificado é revogado, conforme RFC 3647.

5. Controlos de Segurança Física, Gestão e Operacionais

Os controlos e requisitos de segurança física, gestão e operacionais estão estipulados na DP02 – Declaração de práticas da EC da GTS.

6. Controlos de Segurança Técnica

Os controlos de segurança técnica estão estipulados na DP02 – Declaração de práticas da EC da GTS

7. Perfis de Certificado, CRL e OCSP

7.1. Perfil do Certificado

O par de 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 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). 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 para selo eletrónico está de acordo com o conjunto de *standards* ETSI 319 412.

a) Perfil 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)	*RemoteQSCDManagement*		Identificador obrigatório definido no Despacho 155/2017 do GNS
OrganizationUnit (OU)	*Certificado para aplicação*	O	Específico para a faturação eletrónica

Componente do Certificado	Valor	Tipo	Comentários
Subject Alternative Name	<Email do titular>		
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		
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	
[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	

Componente do Certificado	Valor	Tipo	Comentários
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

7.1.1. Número da Versão

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

7.1.2. 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.

7.1.3. Identificadores de Objeto de Algoritmo

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

7.1.4. Formatos de Nome

Consultar ponto 3.1.

7.1.5. Restrições de 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.

7.1.6. OID da Política de Certificado

Todos os certificados emitidos pela PKI GTS contêm os seguintes qualificadores: "*policyQualifIierID*= CPS" e "*cPSuri*", que aponta para o URL onde se encontra a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*".

7.1.7. Utilização de Extensão de Restrições de Política

Não estipulado.

7.1.8. Sintaxe e Semânticas de Qualificadores de Política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores de certificados e autores da política de certificado. O tipo de qualificador é o "*CPSuri*", que contém um apontador, na forma de URL, para a Declaração de Práticas de Certificação publicada pela EC.

7.2. Perfil CRL

7.2.1. Número(s) de Versão

As LRC emitidas contêm os campos básicos e conteúdos específicos na tabela seguinte:

Campo	Valor
Versão	V2
Algoritmo de Assinatura	O algoritmo utilizado pela EC para assinar o certificado é sha256WithRSAEncryption
Emissor	DN da entidade certificadora emissora da LCR
Data Efetiva	A indicação de quando a LCR foi gerada.
Próxima atualização	A indicação de quando será gerada nova LCR.
Certificados Revogados	Lista dos certificados revogados que fornece informação do estado dos certificados no que diz respeito, respetivamente, ao número de série do certificado revogado, a data em que foi revogado e o motivo da sua revogação.

Informação mais detalhada sobre os perfis das LRC pode ser consultada em:

- https://pki.globaltrustedsign.com/index.html
- https://pki02.globaltrustedsign.com/index.html

O perfil dos certificados OCSP pode ser consultado em:

- http://ocsp.globaltrustedsign.com

7.2.2. CRL e Extensões da CRL

Extensão	Valor
Authority Key Identifier	Identificador da EC emissora da CRL
CRL Number	Número sequencial da CRLS

7.3. Perfil OCSP

7.3.1. Número(s) de Versão

Os pedidos e respostas OCSP emitidos pela PKI GTS estão em conformidade com a versão 1 do RFC 6960.