POLÍTICA DE CERTIFICADOS DA ROOT CA GTS

Global Trusted Sign

Referência do Documento | PL11_GTS_V8
Classificação do Documento: Público
Data: 28 de abril de 2021

Índice

1. Introdução 4
1.1 Contexto Geral 4
1.2 Designação e Identificação do Documento 4
Participantes na Infraestrutura de Chave Pública 6
1.4. Utilização do Certificado 6
1.5. Gestão de Políticas 7
1.5.1. Entidade Responsável pela Gestão do Documento 7
1.5.2. Entidade de Contato 7
1.6. Definições e Acrónimos 8
1.6.1. Definições 8
1.6.2. Acrónimos 12
1.6.3. Referências Bibliográficas 13
2. Responsabilidade de Publicação e Repositório 13
3. Identificação e Autenticação 14
3.1 Atribuição de Nomes 14
3.1.1 Tipos de Nomes 14
3.1.2 Necessidade de Nomes Significativos 14
3.1.3 Anonimato ou Pseudónimo de Titulares 14
3.1.4 Interpretação de Formato de Nomes 14
3.1.5 Unicidade de Nomes 14
3.2 Validação da Identidade no Registo Inicial 15
3.2.1 Método de Prova da Posse de Chave Privada 15
3.2.2 Autenticação da Identidade de Pessoa Coletiva 15
3.2.3 Autenticação da Identidade de Pessoa Singular 15
3.2.4 Informação de Subscritor/Titular Não Verificada 15
3.2.5 Validação de Autoridade 15
3.2.6 Critérios para a Interoperabilidade 15
4. Requisitos Operacionais do Ciclo de Vida do Certificado 15
4.1 Pedido de Certificado 15
4.1.1 Quem pode Subscrever um Pedido de Certificado 15
4.1.2 Processo de Registo e Responsabilidades 15
4.2 Processamento do Pedido de Certificado 16
4.2.1. Desempenho de Funções de Identificação e Autenticação 16
4.2.2. Aprovação ou Recusa de Pedidos de Certificado 16
4.2.3. Prazo para Processar o Pedido de Certificado 16
4.3 Emissão de Certificado 16
4.3.1 Procedimentos para a Emissão de Certificado 16
4.3.2 Notificação da Emissão do Certificado ao Titular 16
4.3.3 Procedimentos para a Aceitação do Certificado 16
4.3.4 Publicação do Certificado 16
4.3.5 Notificação da Emissão de Certificado a outras Entidades 17
4.4 Uso do Certificado e Par de Chaves 17
4.4.1 Uso do Certificado e da Chave Privada pelo Titular 17
4.4.2 Uso do Certificado e da Chave Pública pelas Partes Confiantes 17
4.5 Renovação do Certificado com Geração de Novo Par de Chaves 17
4.5.1 Motivo para a Renovação do Certificado com Geração de Novo Par de Chaves 17
4.5.2 Quem pode Submeter o Pedido de Certificado de uma Nova Chave Pública 17
4.5.3 Processamento do Pedido de Renovação do Certificado com Geração de Novo Par de Chaves 17
4.5.4 Notificação da Emissão de Novo Certificado ao Titular 17
4.5.5 Procedimentos para Aceitação de Certificado Renovado com Geração de Novo Par de Chaves 18
4.5.6 Publicação de Certificado Renovado com Geração de Novo Par de Chaves 18
4.5.7 Notificação da Emissão de Certificado Renovado a Outras Entidades 18
4.6 Suspensão e Revogação de Certificado 18
4.6.1 Motivos para a Suspensão 18
4.6.2 Quem pode Submeter o Pedido de Suspensão 18

4.6.3 Procedimentos para Pedido de Suspensão ... 18
4.6.4 Limite do Período de Suspensão ... 18
4.6.5 Motivos para a Revogação ... 18
4.6.6 Quem pode Submeter o Pedido de Revogação ... 19
4.6.7 Procedimento para o Pedido de Revogação ... 19
4.6.8 Produção de Efeitos da Revogação ... 20
4.6.9 Prazo para Processar o Pedido de Revogação ... 20
4.6.10 Requisitos de Verificação da Revogação pelas Partes Confiantes ... 20
4.6.11 Periodicidade da Emissão da Lista de Certificados Revogados ... 20
4.6.12 Período Máximo entre a Emissão e a Publicação da LCR ... 20
4.6.13 Disponibilidade de Verificação Online do Estado / Revogação ... 20
4.6.14 Requisitos de Verificação Online de Revogação ... 20
4.7 Uso do certificado e par de chaves pelo titular ... 21

5. Controlos de Segurança Física, Gestão e Operacionais ... 21

6. Controlos de Segurança Técnica ... 21

7. Perfis de Certificado, CRL e OCSP ... 21

7.1. Perfil do Certificado Auto Assinado da ROOT CA GTS ... 22
7.1.1 Número da Versão ... 23
7.1.2 Extensões do Certificado ... 23
7.1.3 OID do Algoritmo ... 23
7.1.4 Formatos de Nome ... 23
7.1.5 Condicionamento dos Nomes ... 23
7.1.6 OID da Política de Certificado ... 23
7.2 Perfil CRL ... 24
7.2.1 Número(s) de Versão ... 24
7.2.2 CRL e Extensões da CRL ... 24
7.3. Perfil OCSP ... 24
7.3.1. Número(s) de Versão ... 24

1. Introdução

Objetivo

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

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.

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.

1.1 Contexto Geral

O objetivo do presente documento é a definição da 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 de modo a permitir que as partes confiantes e outras entidades ou pessoas interessadas possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

O respetivo documento é elaborado tendo como referência a Declaração de Práticas da Root, DP01_GTS.

1.2 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	8.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.2.1.1.0
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	
08	**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 17:04:35	Tolentino de Deus Faria Pereira Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 06-05-2021 17:07:02	

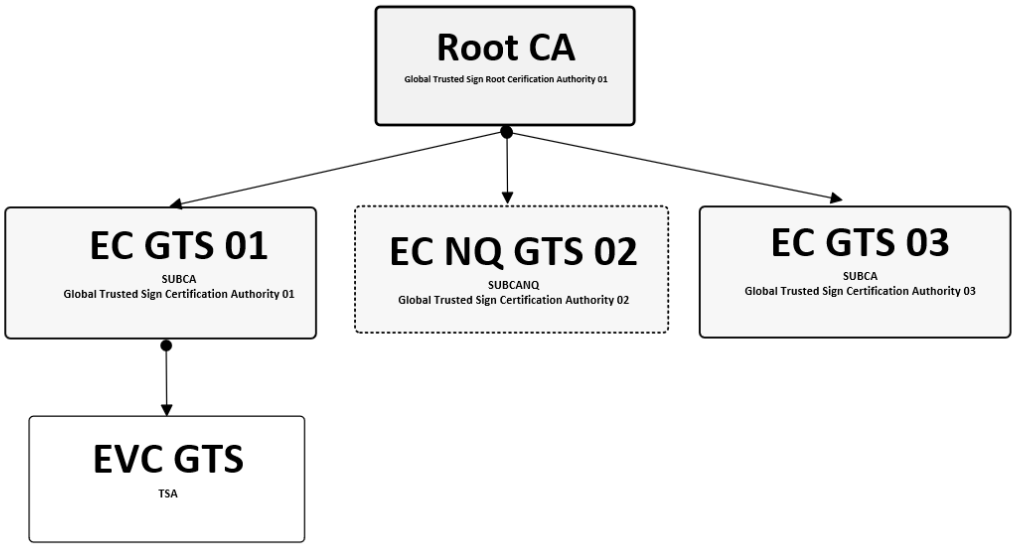
1.2.2. Datas relevantes

Histórico de versões do documento

ID de versão	Data da versão	Motivo de nova versão
Versão 1	31-07-2017	Política de Certificados da Entidade Certificadora Raiz da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014
Versão 2	15-01-2018	Alteração do QtimeStamp - ETSI EN 319 421
Versão 3	31-01-2019	Verificação anual, Alteração dos key usage. Atualização do certificado da TSA
Versão 4	13-12-2019	Atualização com certificado específico de médicos
Versão 5	06-03-2020	Atualização da Arquitetura da TSP
Versão 6	24-06-2020	Adição de certificado de SUBCA 03
Versão 7	17-09-2020	Atualização de registo de colaboradores do Grupo de Confiança da GTS
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**
5 – 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
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

Definições	
Termo	**Definição**
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
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

Definições	
Termo	**Definição**
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
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

Definições	
Termo	**Definição**
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
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

- ✓ DP01_GTS - Declaração de Práticas de Certificação da Root GTS
- ✓ 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 319 411-1: 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 319 412 v1.4.2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
- ✓ ETSI EN 319 401 v2.1.1: Electronic Signatures and Infrastructures (ESI); General policy requirements for Trust Service Providers;
- ✓ RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate and CRL 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.1.7.4.

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 atribuição de nomes segue a convenção determinada pela Declaração de Práticas de Certificação.

3.1.1 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
Country	C	PT
Organization	O	ACIN iCloud Solutions, Lda
Organization Unit	OU	Global Trusted Sign
Common Name	CN	Global Trusted Sign Timestamping Authority 001

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 da Identidade no Registo Inicial

3.2.1 Método de Prova da Posse de Chave Privada

No certificado auto assinado da ROOT CA GTS, a comprovação da posse da chave privada será garantida, através da presença física dos vários Grupos de Trabalho relevantes, na cerimónia de emissão desse tipo de certificados. Nessa cerimónia, será gerado e apresentado o pedido de certificado no formato PKCS#10, cuja assinatura sobre a informação da chave pública será validada.

3.2.2 Autenticação da Identidade de Pessoa Coletiva

Não estipulado.

3.2.3 Autenticação da Identidade de Pessoa Singular

Não estipulado.

3.2.4 Informação de Subscritor/Titular Não Verificada

Toda a informação fornecida pelo subscritor é verificada.

3.2.5 Validação de Autoridade

Não estipulado.

3.2.6 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

4.1.1 Quem pode Subscrever um Pedido de Certificado

Apenas a administração da ACIN ICloud Solutions, Lda. pode subscrever um pedido de certificado auto assinado da ROOT CA GTS.

4.1.2 Processo de Registo e Responsabilidades

O processo de registo do certificado é constituído pelos seguintes passos, a serem efetuados pelos Grupos de Confiança da GTS:

- Geração do par de chaves, publica e privada em ambiente criptográfico apropriado;
- Geração do PKCS#10 correspondente em ambiente criptográfico apropriado.

4.2 Processamento do Pedido de Certificado

O pedido de certificado é processado do seguinte modo:

- Criação do par de chaves e assinatura do certificado em ambiente criptográfico apropriado de acordo com o perfil indicado nesta política;
- Disponibilização do certificado.

4.2.1. Desempenho de Funções de Identificação e Autenticação

A GTS, assim que rececione o 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.

4.2.2. Aprovação ou Recusa de Pedidos de Certificado

Os pedidos de certificados serão aceites, apenas se, todos os dados do pedido forem autênticos.

4.2.3. Prazo para Processar o Pedido de Certificado

Após a aprovação do pedido de certificado, o certificado deverá ser emitido até dez dias úteis.

4.3 Emissão de Certificado

4.3.1 Procedimentos para a Emissão de Certificado

O processo de emissão de certificados é executado pelos Administradores de Registo na ROOT CA GTS através de uma cerimónia própria para o efeito. Os certificados são emitidos por interação da ROOT CA GTS com um módulo criptográfico em *hardware* (*Hardware Secure Module* - HSM). O certificado emitido inicia a sua vigência no momento da sua emissão.

4.3.2 Notificação da Emissão do Certificado ao Titular

A emissão do certificado é efetuada de forma presencial, de acordo com secção anterior. Aceitação do Certificado

4.3.3 Procedimentos para a Aceitação do Certificado

A conclusão da cerimónia de emissão de certificado implica a aceitação formal por parte dos representantes da GTS sobre as funcionalidades e conteúdo do certificado, bem como os direitos e responsabilidades.

4.3.4 Publicação do Certificado

A ROOT CA GTS não efetua a publicação de certificados emitidos.

4.3.5 Notificação da Emissão de Certificado a outras Entidades

A ROOT CA GTS não notifica outras entidades da emissão dos mesmos.

4.4 Uso do Certificado e Par de Chaves

4.4.1 Uso do Certificado e da Chave Privada pelo 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 ROOT CA GTS.

4.4.2 Uso do Certificado e da Chave Pública pelas Partes Confiantes

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

4.5 Renovação do Certificado com Geração de Novo Par de Chaves

Na ROOT CA GTS não existe um processo de renovação de certificado, estando o titular obrigado a fazer um novo pedido de emissão de certificado com os mesmos parâmetros. Este processo obriga a geração de um novo par de chaves, e respetivo certificado. A renovação de certificados utiliza os procedimentos de autenticação e identificação inicial que resultam na geração de novos pares de chaves.

4.5.1 Motivo para a Renovação do Certificado com Geração de Novo Par de Chaves

Não estipulado.

4.5.2 Quem pode Submeter o Pedido de Certificado de uma Nova Chave Pública

Não estipulado.

4.5.3 Processamento do Pedido de Renovação do Certificado com Geração de Novo Par de Chaves

Não estipulado.

4.5.4 Notificação da Emissão de Novo Certificado ao Titular

Não estipulado.

4.5.5 Procedimentos para Aceitação de Certificado Renovado com Geração de Novo Par de Chaves

Não estipulado.

4.5.6 Publicação de Certificado Renovado com Geração de Novo Par de Chaves

Não estipulado.

4.5.7 Notificação da Emissão de Certificado Renovado a Outras Entidades

Não estipulado.

4.6 Suspensão e Revogação de Certificado

A revogação de certificados é o mecanismo a 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 ROOT CA GTS.

4.6.1 Motivos para a Suspensão

Não estipulado.

4.6.2 Quem pode Submeter o Pedido de Suspensão

Não estipulado.

4.6.3 Procedimentos para Pedido de Suspensão

Não estipulado.

4.6.4 Limite do Período de Suspensão

Não estipulado.

4.6.5 Motivos para a 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 ROOT CA GTS;
- Incumprimento por parte da ROOT CA 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.

4.6.6 Quem pode Submeter o Pedido de 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.

4.6.7 Procedimento para o Pedido de Revogação

Os pedidos de revogação do certificado auto assinado da ROOT CA GTS, deverão ser endereçados por escrito ou por mensagem eletrónica assinada digitalmente pela Administração da Acin Icloud Solutions, Lda., indicando o motivo do pedido de revogação. Procede-se, posteriormente à identificação da entidade e ao registo e arquivo do respetivo pedido. Após análise pelo grupo de gestão da GTS, o mesmo fornecerá a informação necessária para a respetiva revogação aos restantes grupos de trabalho. Em qualquer dos casos, é arquivada a descrição pormenorizada de todo o processo de decisão, ficando documentado:

- Data do pedido de revogação;
- Nome do titular do certificado;
- Exposição pormenorizada dos motivos para o pedido de revogação;
- Nome e funções da pessoa que solicita a revogação;
- Informação de contato da pessoa que solicita a revogação;
- Assinatura da pessoa que solicita o pedido de revogação.

4.6.8 Produção de Efeitos da Revogação

A revogação será feita de forma imediata, após terem sido efetuados todos os procedimentos referidos no ponto anterior.

4.6.9 Prazo para Processar o Pedido de Revogação

O pedido de revogação deve ser tratado de forma imediata, pelo que em caso algum poderá ser superior a 24 horas.

4.6.10 Requisitos de Verificação da Revogação pelas Partes Confiantes

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

4.6.11 Periodicidade da Emissão da Lista de Certificados Revogados

A ROOT CA GTS disponibiliza as LRC trimestralmente.

4.6.12 Período Máximo entre a Emissão e a Publicação da LCR

O período máximo entre a emissão e publicação da LCR não deverá ultrapassar os 30 minutos.

4.6.13 Disponibilidade de Verificação Online do Estado / Revogação

A Global Trusted Sign ROOT CA dispõe de serviços de validação OCSP do estado dos certificados de forma online. Esse serviço poderá ser acedido em http://ocsp.globaltrustedsign.com

4.6.14 Requisitos de Verificação Online de Revogação

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). As LRC podem ser acedidas em https://pki.globaltrustedsign.com/index.html, garantindo a sua disponibilidade 24 horas por dia, 7 dias por semana, exceto na ocorrência de alguma paragem de manutenção programada e devidamente comunicada às partes envolvidas. O fim da subscrição de um certificado ocorre quando o prazo de validade é ultrapassado expirado ou o certificado é revogado, conforme RFC 3647.

4.7 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 como a própria Lista de Revogação de Certificados, nos termos definidos na Declaração de Práticas de Certificação.

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

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.509;
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of PubliclyTrusted Certificates.

7.1. Perfil do Certificado Auto Assinado da ROOT CA GTS

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

7.1.1 Número da Versão

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

7.1.2 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.

7.1.3 OID do Algoritmo

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

7.1.4 Formatos de Nome

Consultar ponto 2.1.

7.1.5 Condicionamento dos 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

A extensão *"certificate policeis"* não se encontra ativa no certificado auto assinado da ROOT CA GTS.

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.