

DECLARAÇÃO DE DIVULGAÇÃO DE PRINCÍPIOS DA ENTIDADE CERTIFICADORA RAIZ DA GTS

Global Trusted Sign

Referência do Documento | DP05_GTS_V8

ÍNDICE

1.	Referências.....	3
2.	Documentos Associados	3
3.	Lista de Distribuição.....	3
4.	Histórico do Documento	3
5.	Classificação do Documento	3
6.	Registo da Revisão	3
7.	Introdução.....	4
7.1.	Objetivo	4
7.2.	Público-Alvo.....	4
7.3.	Estrutura do Documento.....	5
8.	Contactos da Entidade Certificadora da ROOT CA GTS	5
9.	Tipos de certificados, procedimentos de validação e utilização.....	6
9.1.	Utilização do Certificado	6
9.2.	Procedimentos de Validação.....	7
10.	Limitação de confiança nos certificados	7
10.1.	Utilização dos certificados.....	7
10.2.	Registos de auditoria	8
11.	Responsabilidades dos Titulares	8
12.	Verificação do Estado dos Certificados emitidos pela ROOT CA GTS.....	9
13.	Limitações e Responsabilidades	10
14.	Acordos, Declaração de Práticas de Certificação e Políticas de Certificação	10
15.	Política de Privacidade.....	10
16.	Legislação Aplicável e Foro Competente	11
17.	Indemnizações	11
18.	Legislação e Normas	11
19.	Auditorias e Normas de Segurança	11
20.	Acrónimos	12

<p>1. Referências</p>	<p>Regulamentação Europeia Nº 910/2014 ETSI 319 411-1 ETSI 319 412 ETSI 319 401 RFC 5280: Internet X.509 PKI - Certificate and CRL Profile, 2008 CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.7; ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, v2.4.1</p>
<p>2. Documentos Associados</p>	<p>DP01_GTS - Declaração de Práticas de Certificação da Root CA GTS PL11_GTS – Política de Certificados da Root CA GTS</p>
<p>3. Lista de Distribuição</p>	<p>Partes interessadas da hierarquia de confiança da GTS</p>
<p>4. Histórico do Documento</p>	<p>31-07-2017 Versão 1 16-04-2018 Versão 2 02-05-2020 Versão 3 24-06-2020 Versão 4 23-09-2020 Versão 5 04-10-2021 Versão 6 22-07-2022 Versão 7 15-02-2023 Versão 8</p>
<p>5. Classificação do Documento</p>	<p>D Público</p>

6. Registo da Revisão

N.º da Versão	Elaborado	Aprovado	Motivo
8	15-02-2023	15-02-2023	Atualização de hierarquia do PKI e revisão do documento
	<p>SegAdm Hélder Lino de Abreu Vieira</p>	<p>Grupo de Gestão Tolentino de Deus Faria Pereira</p>	

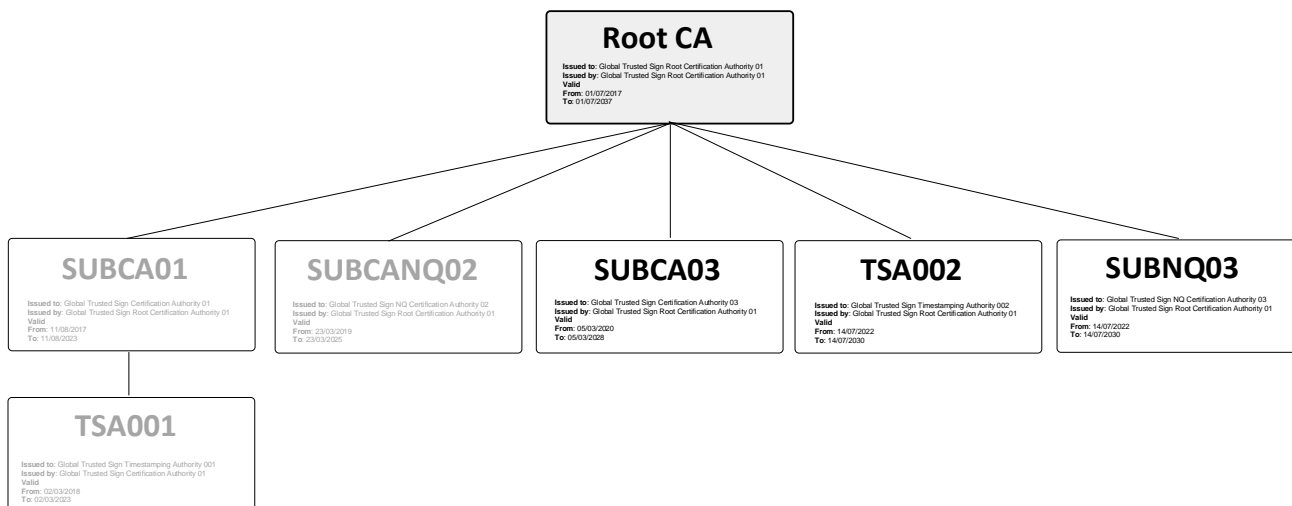
7. Introdução

7.1. Objetivo

Este documento pretende resumir, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Políticas de Certificação da Infraestrutura de chave pública da Entidade de Certificação Raiz da Global Trusted Sign (adiante designada por Entidade Certificadora ROOT da GTS ou ROOT CA GTS).

A infraestrutura da ROOT CA GTS fornece uma hierarquia de confiança, que promove a segurança eletrónica do titular do certificado digital. A ROOT CA GTS estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A ROOT CA GTS é uma entidade certificadora credenciada pelo Gabinete Nacional de Segurança (<http://www.gns.gov.pt/trusted-lists.aspx>), conforme previsto na legislação portuguesa e europeia, encontrando-se assim legalmente habilitada a emitir diversos tipos de certificados digitais. A ROOT CA GTS representa a raiz da hierarquia de confiança, representada na seguinte figura:



Legenda:

- 1 – Root CA GTS - Entidade Certificadora Raiz da GTS
- 2 – SUBCA01 - Entidade Certificadora
- 3 – TSA001 - Entidade Certificadora de Validação Cronológica da GTS
- 4 – SUBCANQ02 - Entidade Certificadora Não Qualificada da GTS
- 5 – SUBCA03 – Entidade Certificadora da GTS
- 6 – TSA002 – Entidade Certificadora de Validação Cronológica da GTS
- 7 – SUBNQ03 – Entidade Certificadora Não Qualificada da GTS

7.2. Público-Alvo

O presente documento deve ser lido pelos titulares e futuros subscritores de certificados emitidos pela ROOT CA GTS.

7.3. Estrutura do Documento

O presente documento encontra-se organizado em conformidade com a norma ETSI EN 319 411-1.

O presente documento é a Declaração de Divulgação de Princípios da ROOT CA GTS cujo OID associado é 1.3.6.1.4.1.50302.1.1.3.1.1.0, enquanto o OID associado à Política de Certificados da ROOT CA GTS é 1.3.6.1.4.1.50302.1.1.2.1.1.0:

Informação do Documento	
Nome do Documento	Declaração de Divulgação de Princípios da ROOT CA GTS
Versão do Documento	8.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.3.1.1.0
Data de Emissão	15 de fevereiro de 2023
Validade	15 de fevereiro de 2024
Localização	https://pki.globaltrustedsign.com/index.html

Nota: Atualizações regulares neste documento são realizadas sempre que se justificarem.

8. Contactos da Entidade Certificadora da ROOT CA GTS

Nome	Grupo de Confiança da GTS
Gestores	Tolentino de Deus Faria Pereira José Luís de Sousa
Morada	ACIN iCloud Solutions, Lda. Estrada Regional 104 N°42-A 9350-203 Ribeira Brava Madeira – Portugal
E-mail geral	info@globaltrustedsign.com
E-mail reportes	report@globaltrustedsign.com
Página de Internet	https://www.globaltrustedsign.com
Telefone	Nacional: 707 451 451 Internacional: + 351 291 957 888 (Opção 1 – Português / opção 2 – Inglês; Opção 6 – GTS)

Sempre que se identifiquem alguns dos motivos para revogação devem ser comunicados para os contactos supra ou preferencialmente para o e-mail de reportes.

A ROOT CA GTS não suporta a suspensão de certificados.

9. Tipos de certificados, procedimentos de validação e utilização

9.1. Utilização do Certificado

Os certificados emitidos na hierarquia de confiança da ROOT CA GTS são utilizados, pelos diversos sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança:

- a) Confidencialidade;
- b) Integridade;
- c) Autenticação;
- d) Não-repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a ROOT CA GTS proporciona. Assim, os serviços de identificação, autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves.

9.1.1. Utilização Adequada

Os certificados emitidos pela ROOT CA GTS são regulamentados por esta Declaração de Práticas de Certificação e serão utilizados de acordo com a função e finalidade estabelecida nas Declarações de Práticas de Certificação e nas correspondentes Políticas de Certificados, de acordo com a lei em vigor.

As Partes Confiantes podem verificar a cadeia de confiança de um certificado emitido pela ROOT CA GTS, garantindo assim a autenticidade e identidade do titular.

9.1.2. Utilização não autorizada

Os certificados emitidos na hierarquia de confiança da ROOT CA GTS não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente, ressalvada a exceção de poderem ser utilizados em outros contextos quando legalmente previstos na legislação aplicável.

Os serviços qualificados de confiança oferecidos pela ROOT CA GTS, não foram desenhados e como tal não estão autorizados para utilização em atividades de alto risco ou que requeiram uma atividade isenta de falhas, designadamente as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

9.2. Procedimentos de Validação

Os certificados qualificados para autenticação de sítios Web emitidos pela ROOT CA GTS são confiáveis no espaço público e cumprem com o estipulado nos seguintes documentos:

- Declaração de Práticas de Certificação da ROOT CA GTS:
 - Define as práticas seguidas pela ROOT CA GTS para a gestão do ciclo de vida dos certificados (OID: 1.3.6.1.4.1.50302.1.1.1.1.1.0)
- Políticas de Certificados da ROOT CA GTS:
 - Define o perfil dos Certificados de Entidades Certificadoras (OID: 1.3.6.1.4.1.50302.1.1.2.1.1.0)

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.

10. Limitação de confiança nos certificados

10.1. Utilização dos certificados

A utilização dos certificados emitidos para os titulares deve obedecer ao descrito nas respetivas políticas de certificados disponíveis em <https://www.pki.globaltrustedsign.com/index.html>.

Os certificados emitidos pela ROOT CA GTS são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido pelas entidades certificadoras subordinadas da hierarquia de confiança da ROOT CA GTS, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado.

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pela legislação aplicável.

Os certificados emitidos pela ROOT CA GTS não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços qualificados de confiança oferecidos pela ROOT CA GTS, não foram concebidos nem estão autorizados a ser utilizados em atividades de alto risco ou que necessitem uma atividade isenta de falhas, como:

- Funcionamento de instalações hospitalares;
- Funcionamento de instalações nucleares;
- Controlo de tráfego aéreo;
- Controlo de tráfego ferroviário;

- Ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

10.2. Registos de auditoria

Dos eventos significativos geradores de registos auditáveis são considerados os seguintes:

- Eventos relacionados com segurança, incluindo:
 - Tentativas de acesso (com e sem sucesso) a recursos sensíveis da ROOT CA GTS;
 - Operações realizadas por membros dos Grupos de Trabalho;
 - Dispositivos físicos de segurança de entrada / saída dos vários níveis de segurança.
- Pedidos de emissão de certificados;
- Atualização das LRC;

As entradas nos registos incluem a informação seguinte:

- Categoria do evento;
- Data e hora do evento;
- Descrição do evento;
- Identidade do sujeito que causou o evento;
- Número de série do evento.

Os registos de auditoria são mantidos disponíveis durante pelo menos 1 mês após processamento, e depois arquivados em conformidade com a legislação nacional.

11. Responsabilidades dos Titulares

Os titulares de certificados utilizarão a sua chave privada apenas e só para fim a que estas se destinam (conforme estabelecido no campo do certificado *keyUsage*) e sempre com propósitos legais. A utilização dos certificados apenas é permitida:

- A quem estiver designado no campo *Subject* do certificado e,
- Enquanto o certificado se mantiver válido (estado ativo) e não estiver na LRC da ROOT CA GTS.

O titular do certificado deve solicitar a revogação de um determinado certificado, sempre que haja conhecimento ou suspeita do comprometimento da respetiva chave privada, ou qualquer outro ato que recomende esta ação. A ROOT CA GTS guarda toda a documentação utilizada para a verificação da identidade e autenticidade da entidade que efetua o pedido de revogação.

Um certificado pode ser revogado, se alguma das seguintes condições se verificar:

- Comprometimento ou suspeita de comprometimento da chave privada ou da senha de acesso à chave privada;
- Perda da chave privada;
- Imprecisões graves nos dados fornecidos;
- Comprometimento ou suspeita de comprometimento da chave privada da ROOT CA GTS;
- Incumprimento por parte da Entidade de Certificação ou titular das responsabilidades previstas;
- Sempre que existam razões credíveis que indiquem 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.

Na utilização do certificado e da respetiva chave pública, o titular deve ser garantir o cumprimento das seguintes condições:

- Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública;
- Ser responsável pela sua correta utilização;
- Ler e entender os termos e condições descritos nas Políticas e práticas de certificação;
- Verificar e validar a cadeias de confiança dos certificados;
- Verificar as Listas de Revogação de Certificados (LRC) tendo especial atenção às suas extensões marcadas como críticas e propósito do certificado (*keyUsage*) em questão;
- Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

12. Verificação do Estado dos Certificados emitidos pela ROOT CA GTS

Outras partes que confiam nos certificados emitidos pela ROOT CA GTS devem:

- Utilizar os mecanismos de consulta das LRC indicadas anteriormente, e verificar o estado do certificado no momento da sua utilização. É da sua responsabilidade essa verificação;
- Obedecer ao especificado nas Políticas de Certificado do certificado em causa (<https://www.pki.globaltrustedsign.com/index.html>);
- Utilizar o certificado adequadamente de acordo com os objetivos da sua emissão.

13. Limitações e Responsabilidades

A ROOT CA GTS:

- a) Responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Art.º 26 do DL 62/2003.
- b) Responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão do serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele.
- c) Assume a responsabilidade sobre os riscos que os particulares sofram sempre que sejam consequência do normal, ou anormal funcionamento dos seus serviços.
- d) Apenas responde pelos danos e prejuízos causados pelo uso indevido de certificados reconhecidos quando os limites quanto ao possível uso não estejam definidos nos certificados, de forma clara reconhecida por terceiros.
- e) Não responde quando o titular superar os limites que figuram no certificado quanto às suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular.
- f) Não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações.
- g) Não assume qualquer responsabilidade no caso de perda ou prejuízo:
 - o Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro motivo de força maior.
 - o Proporcionados pelo uso dos certificados quando estes excedam os limites estabelecidos pelos mesmos na Política de Certificados e Declaração de Práticas de Certificação.
 - o Proporcionados pelo uso indevido ou fraudulento dos certificados ou das LRCs emitidas por ela.

14. Acordos, Declaração de Práticas de Certificação e Políticas de Certificação

Todos os acordos aplicáveis, Declarações de Práticas de Certificação, Políticas de Certificado e Política de Privacidade encontram-se disponíveis em <https://www.pki.globaltrustedsign.com/index.html>.

15. Política de Privacidade

A ROOT CA GTS implementa medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa, garantindo que a informação do titular, solicitada para a emissão dos

respetivos certificados digitais, não se encontra publicada sendo processada de acordo com as Políticas de Certificados da ROOT CA GTS.

16. Legislação Aplicável e Foro Competente

Qualquer litígio decorrente da interpretação ou aplicação deste documento regem-se pela lei portuguesa. Para regular esses litígios, as partes elegem o foro judicial da Comarca de Funchal, com exclusão de qualquer outro.

17. Indemnizações

A ROOT CA GTS assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável em vigor.

18. Legislação e Normas

A ROOT CA GTS exerce a sua atividade de emissão de certificados de acordo com as seguintes normas/regulamentos:

- 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 do Parlamento Europeu e do Conselho de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas)
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers, e os standards relacionados com os serviços qualificados de confiança
- Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

19. Auditorias e Normas de Segurança

Todas as intervenções realizadas à ROOT CA GTS são validadas por auditores internos. A ROOT CA GTS é auditada por um auditor independente da esfera de influência da Entidade de Certificação, sendo esta independência uma exigência pela Entidade Supervisora. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, à Entidade Supervisora.

20. Acrónimos

OSCP	<i>Online Certificate Status Protocol</i>
LRC	Lista de Revogação de Certificados
VPN	<i>Virtual Private Network</i>
EC	Entidade de Certificação
DL	Decreto Lei
DPC	Divulgação de Princípios de Certificação
UE	União Europeia