DECLARAÇÃO DE DIVULGAÇÃO DE PRÍNCIPIOS DA ENTIDADE CERTIFICADORA DA GTS

Global Trusted Sign

Referência do Documento | DP04_GTS_V10

ÍNDICE

1. Referências	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
2. Documentos Associados	DP02_GTS - Declaração de Práticas de Certificação da EC GTS PL01_GTS - Política de Certificados para Assinatura Qualificada PL02_GTS - Política de Certificados para Selo_Eletrónicos PL03_GTS - Política_de_Certificados_SSL_EV_Indice PL04_GTS - Política_de_Certificados_SSL_OV_indice PL16_GTS - Política de Certificados para Assinaturas Avançadas PL17_GTS - Política de Certificados para Selos Eletrónicos Avançados
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	01-07-2017 | Versão 1 29-12-2017 | Versão 2 16-04-2018 | Versão 3 05-04-2019 | Versão 4 04-05-2020 | Versão 5 24-06-2020 | Versão 6 17-09-2020 | Versão 7 04-10-2021 | Versão 8 20-07-2022 | Versão 9 15-02-2023 | Versão 10
5. Classificação do Documento	D | Público

6. Registo da Revisão

N.º da Versão	Elaborado	Aprovado	Motivo
	15-02-2023	15-02-2023	
10	**AdmSeg**	**Grupo de Gestão**	Atualização da hierarquia do PKI e revisão do documento.
	Hélder Lino de Abreu Vieira	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: HELDER LINO DE ABREU VIEIRA Data: 15-02-2023 11:38:41		

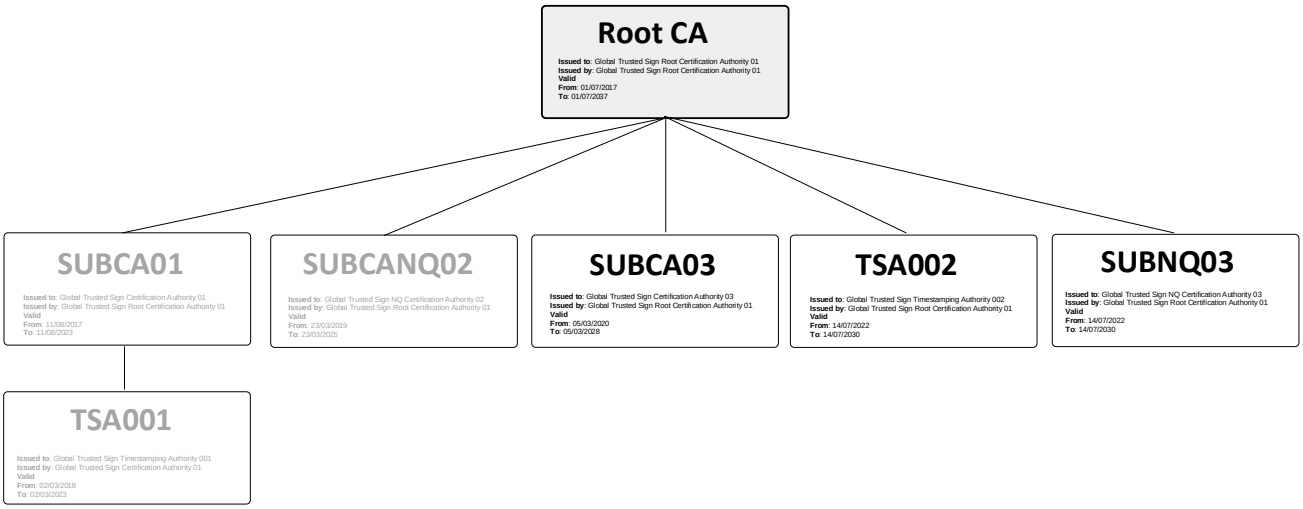
7. Introdução

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 da Global Trusted Sign (adiante designada por Entidade Certificadora da GTS ou EC GTS).

A infraestrutura da EC GTS fornece uma hierarquia de confiança, que promove a segurança eletrónica do titular do certificado digital. A EC 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 Entidade Certificadora da GTS (EC 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 EC GTS é assinada pela Root CA GTS, inserindo-se assim numa 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 EC 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 EC GTS cujo OID associado é 1.3.6.1.4.1.50302.1.1.3.2.1.0, enquanto os OID associado às Políticas de Certificados da EC GTS encontram-se referenciados no ponto 9.2:

Informação do Documento	
Nome do Documento	Declaração de Divulgação de Princípios da EC GTS
Versão do Documento	10.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.3.2.1.0
Data de Emissão	15 de fevereiro de 2023
Validade	15 de fevereiro de 2024
Localização	https://pki.globaltrustedsign.com/index.html

Nota: As atualizações realizadas a este documento são realizadas sempre que existam alterações aos procedimentos, legais ou estatais, ou sempre que se justifique.

8. Contactos da Entidade Certificadora da 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 Nº42-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

9. Tipos de certificados, procedimentos de validação e utilização

9.1. Utilização do Certificado

Os certificados qualificados de autenticação de sítios Web emitidos pela EC GTS são utilizados pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de estabelecer comunicação de dados Web através de protolocos SSL/TLS.

Garantem-se assim comunicações eletrónicas eficientes e seguras, ao mesmo tempo que a preocupação dos utilizadores com a confiança dos certificados é endereçada.

9.1.1. Utilização Adequada

Os requisitos e regras definidas neste documento aplicam-se a todos os certificados emitidos pela EC GTS. Estes certificados têm como objetivo:

- Identificar a entidade coletiva que controla um sítio web: fornece garantia razoável ao utilizador de um navegador Internet que o sítio web que o utilizador está a aceder é controlado por uma entidade coletiva que está identificada no certificado através do nome, sede social, inscrição no Instituto de Registos e Notariado, ou outra informação desambiguadora.

- Permitir comunicações cifradas com um sítio Web: facilita a troca de chaves de cifra de modo a permitir a comunicação de informação cifrada através da Internet, entre o utilizador de um navegador Internet e um sítio web.

Ao fornecer um processo de verificação de identidade mais fiável e informação da sede social da empresa, os certificados de *Extended Validation* (EV) podem ajudar a:

- Dificultar os ataques de phishing e outros de fraude de identidade que utilizam certificados

- Apoiar as empresas que possam ter sido o alvo de um ataque de phishing ou fraude de identidade ao disponibilizar uma ferramenta para a sua identificação perante os utilizadores

- Apoiar as forças de segurança nas suas investigações de phishing e outros ataques de fraude de identidade, apoiando, quando aplicável, o contacto, investigação, e ações legais contra o Titular.

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

9.1.2. Utilização não autorizada

Os certificados qualificados para autenticação de sítios Web emitidos pela EC GTS estão focados na identidade do Titular do certificado, e não no seu comportamento. Deste modo, um certificado de autenticação Web não dá quaisquer garantias sobre:

- O Titular identificado no certificado está efetivamente a prestar serviço;
- O Titular identificado no certificado está em conformidade com a legislação aplicável;
- Titular identificado no certificado é confiável, honesto ou ético na execução do seu negócio;
- Que é "seguro" estabelecer uma relação comercial com o Titular identificado no certificado.

9.2. Procedimentos de Validação

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

- Declaração de Práticas de Certificação da EC GTS:
    - Define as práticas seguidas pela EC GTS para a gestão do ciclo de vida dos certificados (OID: 1.3.6.1.4.1.50302.1.1.1.2.1.0)
- Políticas de Certificados da EC GTS:
    - SSL EV: define o perfil dos Certificados de Autenticação de Sítios Web com Extended Validation (OID: 1.3.6.1.4.1.50302.1.1.2.2.1.0)
    - SSL OV: define o perfil dos Certificados de Autenticação de Sítios Web com Organization Validation (OID: 1.3.6.1.4.1.50302.1.1.1.2.1.1)
    - Assinaturas Qualificadas: define o perfil dos certificados qualificados de assinatura para pessoa singular, pessoa singular com associação profissional, pessoa coletiva, pessoa coletiva com associação profissional e de médico (OID: 1.3.6.1.4.1.50302.1.1.1.2.1.2)
    - Selos eletrónicos: define o perfil dos certificados qualificados de selo eletrónico e selo eletrónico para faturação (OID: 1.3.6.1.4.1.50302.1.1.1.2.1.3)
    - Assinaturas avançadas: define o perfil dos certificados avançados de assinatura para pessoa singular, pessoa singular com associação profissional, pessoa coletiva, pessoa coletiva com associação profissional (OID: 1.3.6.1.4.1.50302.1.1.2.6.1.0)
    - Selos avançados: define o perfil dos certificados avançados de selo eletrónico (OID: 1.3.6.1.4.1.50302.1.1.2.7.1.0)

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 EC GTS são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido pela EC 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 EC GTS não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços qualificados de confiança oferecidos pela EC 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 EC 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 EC 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 EC GTS guarda toda a documentação utiliza 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 EC GTS ou da Root CA GTS;
- Incumprimento por parte da Entidade de Certificação ou titular das responsabilidades previstas;
- Sempre que existam razões credíveis que indiciem 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 EC GTS

Outras partes que confiam nos certificados emitidos pela Entidade de Certificação da 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 EC 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 perca ou prejuízo:

- Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro motivo de força maior.
- Proporcionados pelo uso dos certificados quando estes excedam os limites estabelecidos pelos mesmos na Política de Certificados e Declaração de Práticas de Certificação.
- 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 EC 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 EC GTS assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável em vigor.

18. Legislação e Normas

A EC 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
- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4
- 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 Entidade de Certificação da GTS são validadas por auditores internos. A Entidade de Certificação da 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	*Online Certificate Status Protocol*
LRC	Lista de Revogação de Certificados
VPN	*Virtual Private Network*
EC	Entidade de Certificação
DL	Decreto Lei
DPC	Divulgação de Princípios de Certificação
UE	União Europeia