DECLARAÇÃO DE DIVULGAÇÃO DE PRÍNCIPIOS DA ENTIDADE DE VALIDAÇÃO CRONOLÓGICA DA GTS

Global Trusted Sign

Referência do Documento | DP06_GTS_V9

ÍNDICE

1. Referências	Regulamentação Europeia Nº 910/2014 CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.5; RFC 3161 – Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP) ETSI 319 421 ETSI 319 422 ETSI 319 401
2. Documentos Associados	DP03_GTS - Declaração de Práticas de Certificação da EVC GTS PL14_GTS - Política de Certificados para Selos Temporais
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	31-07-2017 | Versão 1 16-02-2018 | Versão 2 01-06-2018 | Versão 3 10-03-2020 | Versão 4 24-06-2020 | Versão 5 17-09-2020 | Versão 6 04-10-2021 | Versão 7 22-07-2022 | Versão 8 15-02-2023 | Versão 9
5. Classificação do Documento	D | Público

6. Registo da Revisão

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	15-02-2023	**15-02-2023**	
9	**AdmSeg**	**Grupo de Gestão**	Atualização da hierarquia do PKI e revisão do documento.
	Hélder Lino de Abreu Viera	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: HELDER LINO DE ABREU VIEIRA Data: 15-02-2023 11:38:40		

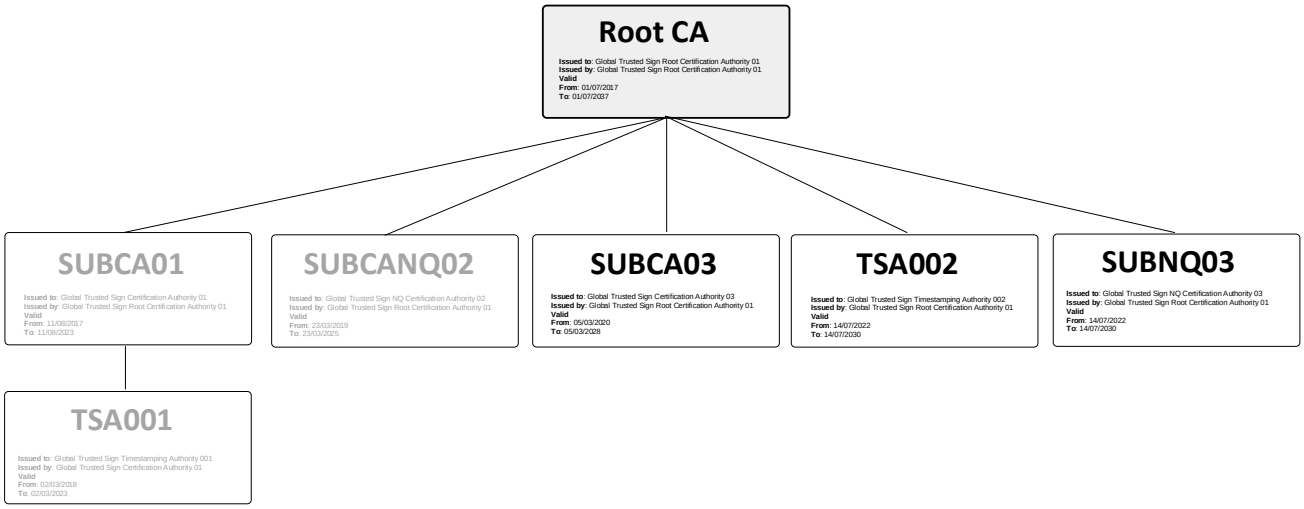
7. Introdução

7.1. Objetivo

Este documento pretende resumir, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Práticas de Validação Cronológica da Entidade de Validação Cronológica da Global Trusted Sign (adiante designada por EVC GTS), no que diz respeito à emissão de selos temporais e disponibilização de mecanismos de validação cronológica.

A infraestrutura da EVC GTS fornece uma hierarquia de confiança, que promove a segurança eletrónica do titular do selo temporal. A EVC 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 EVC 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 EVC 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 selos temporais emitidos pela EVC GTS.

7.3. Estrutura do Documento

O presente documento encontra-se organizado em conformidade com a norma ETSI EN 319 421.

O presente documento é a Declaração de Divulgação de Princípios da Validação Cronológica da EVC GTS cujo OID associado é: 1.3.6.1.4.1.50302.1.1.3.3.1.0, enquanto que o OID de boas práticas associado à Política de Certificados de Validação Cronológica é 0.4.0.2023.1.1 (conforme definido pela ETSI EN 319 421) e o identificador único da Política de Certificados de Validação Cronológica é o 1.3.6.1.4.1.50302.1.1.2.3.1.0.

Este documento é identificado pelos dados constantes na seguinte tabela:

Informação do Documento	
Nome do Documento	Declaração de Divulgação de Princípios da Validação Cronológica da EVC GTS
Versão do Documento	9.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.3.3.1.0
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 justifiquem.

8. Contactos da Entidade Certificadora 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 Selos Temporais e Utilização

A EVC GTS tem como objetivo fornecer serviços de emissão de selos temporais qualificados de acordo com 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. O algoritmo de assinatura suportado é o sha256WithRSAEncryption (comprimento da chave de 4096 bits).

Os selos temporais são emitidos a pedido dos subscritores, de acordo com a norma ETSI EN 319 421 e cumprem os requisitos impostos pela RFC 3161.

A TSU da EVC GTS assina digitalmente os selos temporais dando uso a certificados digitais, cada um com uma validade de cinco anos. Durante esse período após a emissão do selo temporal, a validade do selo pode ser verificada, calculando o prazo entre a data de emissão e os 5 anos de validade.

10. Limites de confiança

O objetivo dos selos temporais é garantir que um documento (ou ficheiro) existia num determinado momento no tempo. Esta garantia é obtida através da geração de um selo temporal qualificado emitido por uma entidade certificadora credenciada (como a EVC GTS) associado ao *hash* do documento ao qual será feita a aposição do selo temporal.

Deste modo, a associação de um selo temporal ao documento certifica não só a veracidade da hora e data do pedido, mas também a integridade e não repúdio do conteúdo.

Os selos temporais emitidos pela EVC GTS de acordo com esta DPC são certificados qualificados em conformidade com os requisitos do regulamento (EU) 910/2014.

Os selos temporais emitidos pela EVC GTS são confiáveis no espaço público e cumprem com o estipulado nos seguintes documentos:

- Declaração de Práticas de Certificação da EVC GTS:
    - Define as práticas seguidas pela EVC GTS para a gestão do ciclo de vida dos certificados (OID: 1.3.6.1.4.1.50302.1.1.1.3.1.0)
- Políticas de Certificados da EVC GTS: OID = 1.3.6.1.4.1.50302.1.1.2.3.1.0

A EVC GTS garante que o(s) relógio(s) que fornecem a hora/data (timestamp) incluída no selo temporal estão sincronizados uma precisão mínima de 1 segundo em relação ao UTC.

São mantidos registos (logs) da EVC GTS durante um mínimo de 7 anos, estando neste período de tempo disponíveis como evidência de suporte à precisão indicada nos selos temporais emitidos.

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.

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. Validação Cronológica

12.1. Emissão do selo temporal

O selo temporal é emitido de forma segura e de acordo com as recomendações da norma ETSI EN 319 422 com uma hora/data (timestamp) correta, possuindo os parâmetros seguintes:

- O identificador da política usada para a geração do selo temporal (0.4.0.2023.1.1)
- Um *timestamp*;
- Um *hash* criptográfico dos dados junto com o *timestamp*;
- Um serial number único;
- Um selo eletrónico gerado com a chave privada da EVC GTS, dedicada para esta função;
- Uma precisão mínima de 1 segundo em relação ao UTC, cuja sincronização de tempo da EVC GTS é feita com o servidor de tempo disponibilizado pelo Observatório Astronómico de Lisboa.

12.2. Sincronização do relógio

Para efetuar a sincronização UTC necessária para a emissão de selos temporais é usado um relógio atómico com ligação GPS (Global Positioning System). Para satisfazer os requisitos de redundância impostos pela norma ETSI EN 319 412, foram configuradas mais duas fontes de tempo conforme imposto pela mesma norma. As fontes redundantes de tempo consideradas são:

- Royal Observatory of Belgium (ORB), Belgica, Bruxelas - ntp1.oma.be
- Observatoire de Paris (LNE-SYRTE), Paris, France - ntp-p1.obspm.fr

12.3. Processamento do pedido de selo temporal

O subscritor efetua o pedido de selo temporal, cujo processamento é feito de imediato pela EVC e de forma automática de acordo com os limites indicados neste documento.

Em caso de perda de sincronismo dos serviços de validação cronológica, a EVC GTS não emitirá selos temporais até que seja reposto o estado normal de operação.

Em caso de comprometimento ou suspeita de comprometimento dos serviços de validação cronológica, a EVC GTS não emitirá selos temporais até que seja reposto o estado normal de operação.

12.4. Utilização adequada

Os selos temporais são emitidos a pedido dos subscritores e de acordo com o RFC 3161.

São também utilizados pelas Partes Confiantes para validação da associação da data/hora ao datum, devendo para tal:

- Verificar que o selo temporal foi corretamente assinado e que a chave privada utilizada para assina o selo temporal não foi comprometida até ao momento da verificação. Durante a validade do certificado da TSU, a validade da chave de assinatura pode ser verificada através da verificação do estado de revogação do certificado da TSU;
- Ter em consideração as limitações à utilização do selo temporal conforme definido nesta declaração de práticas e na política de certificados;
- Ter em consideração quaisquer outras precauções aplicáveis à utilização do selo temporal definida, por exemplo, em acordos.

Nota: Os requisitos e regras definidos neste documento aplicam-se a todos os selos temporais emitidos pela EVC GTS.

12.5. Utilização não autorizada

Os selos temporais não podem ser utilizados para qualquer função fora do âmbito das utilizações descritas na secção anterior e da legislação aplicável.

13. Limitações e Responsabilidades

A EVC 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://pki.globaltrustedsign.com/index.html.

15. Política de Privacidade

A EVC GTS implementa medidas que garantem a privacidade dos dados pessoais, de acordo com o regulamento geral de proteção de dados (regulamento 2016/679), garantindo que a informação do titular, solicitada para a emissão dos respetivos selos temporais, não se encontra publicada sendo processada de acordo com as Políticas de Certificados da ROOT CA GTS e com a Política de Privacidade da 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 EVC GTS assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável em vigor.

18. Legislação e Normas

A EVC GTS exerce a sua atividade de emissão de selos temporais 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 319 421 - Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers
- 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 Validação Cronológica da GTS é auditada por um auditor independente da

esfera de influência da Entidade Certificadora, sendo esta independência uma exigência pela Entidade Supervisora. A sua missão é auditar a infraestrutura da Entidade de Validação Cronológica, 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

Assinado com Assinatura Digital Qualificada por:
TOLENTINO DE DEUS FARIA PEREIRA
Data: 15-02-2023 15:44:21