multicert

Engineering for digital security

Declaração de Divulgação da TSA

Política

MULTICERT_PJ.CA3_24.1.13_0001_pt

Identificação do Projeto: TSA da Multicert

Nível de Acesso: Público

Versão: 3.0

Data: 31/03/2022

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edifício 3, Piso 3 - 2740-266 Porto Salvo – Oeiras
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

Identificador do documento: MULTICERT_PJ.CA3_24.1.13_0001_pt

Palavras-chave: SVC, Time-Stamping, Declaração de Divulgação da TSA

Tipologia documental: Política

Título: Declaração de Divulgação de Princípios de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 31/03/2022

Versão atual: 3.0

Identificação do Projeto: TSA da Multicert

Identificação da CA: PKI da MULTICERT

Cliente: --

Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	04/08/2009	Versão inicial	MULTICERT S.A.
1.1	07/08/2009	Atualização de Conteúdos	MULTICERT S.A.
1.2	24/08/2009	Correções gerais	MULTICERT S.A.
1.3-1.4	06/06/2014	Atualização de Conteúdos	MULTICERT S.A.
2.0	01/08/2014	Versão Aprovada	MULTICERT S.A.
2.1	22/11/2016	Atualização de conteúdo de acordo com conformidade	MULTICERT S.A.
2.2-2.3	26/11/2018	Atualização de conteúdo de acordo com conformidade	MULTICERT S.A.
2.4	05/01/2022	Revisão de conteúdo	MULTICERT S.A.
3.0	31/03/2022	Versão Aprovada	MULTICERT S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_427	Declaração de Práticas de Certificação MULTICERT	MULTICERT S.A.
MULTICERT_PJ.CA3_24.1.1_0002_pt	Declaração de Práticas de Validação Cronológica	MULTICERT S.A.

Sumário

1 Declaração de Divulgação da TSA

Este documento constitui a Declaração de Divulgação da TSA da Multicert.

Nesta secção, a Entidade de Validação Cronológica da Multicert (EVC ou TSA – Time-stamping Authority) divulga a todos os seus Subscritores e potenciais Partes Confiantes (*Relying Parties*), um resumo dos termos e condições de utilização dos serviços de validação cronológica, numa linguagem acessível e de fácil compreensão.

Este documento não deverá ser visto como um resumo de todas as práticas e políticas seguidas pela TSA, mas como um resumo de alguns dos pontos mais importantes, pelo que a leitura deste documento deve ser complementada com a leitura da Declaração de Práticas de Validação Cronológica – DPVC – (disponível em https://pki.multicert.com).

1.1 Informação de Contato da TSA

Os serviços e repositório da TSA da Multicert estão disponíveis através dos seguintes meios de comunicação:

NOME	Grupo de Trabalho de Autenticação da PKI da Multicert
Morada	A/C: Grupo de Trabalho de Autenticação Multicert – Serviços de Certificação Electrónica, S.A. Lagoas Park, Edifício 3, Piso 3 2740-266 Porto Salvo – Oeiras, Portugal
Correio eletrónico	ca.forum@multicert.com
Página Web	https://www.multicert.com
Repositório	https://pki.multicert.com
Telefone	+351 217 123 010

1.2 Tipo de Selo Temporal e Utilização

A TSA da Multicert emite selos temporais qualificados de de acordo com as regras e requisitos do Regulamento (UE) nº 910/2014 [11],sendo identificado pelos seguintes OID`s:

- 1.3.6.1.4.1.25070.1.2.1.0.1 – identificador de Declaração de Práticas de Validação Cronológica
- 1.3.6.1.4.1.25070.1.1.1.0.7 – identificador de Declaração de Práticas de Certificação da Multicert

Ao incluir este identificador, a Multicert indica conformidade com as seguintes políticas de selo temporal adicionais:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023)

policy-identifiers(1) best-practices-ts-policy (1)

Os seguintes identificadores são descontinuados, mas a sua informação passa a estar presente na Declaração de Práticas de Validação Cronológica e Declaração de Práticas de Certificação da Multicert cujos OID`s se encontram acima referidos:

- 1.3.6.1.4.1.25070.1.1.1.2.0.1.1
- 1.3.6.1.4.1.25070.1.1.1.2.0.7

A TSA da Multicert aceita pedidos de selo temporal dos seus Subscritores/Titulares, de acordo com o RFC 3161 [13]. O algoritmo de *hash* utilizado para representar o *datum* ao qual se vai apor o selo temporal é o SHA-256.

O selo temporal é assinado digitalmente pela TSU da TSA da Multicert, por um certificado digital com um período mínimo de cinco anos de validade. Durante o período de validade do certificado da TSU, a validade da chave privada de assinatura pode ser verificada através do estado de revogação do certificado, consultando o OCSP ou CRL disponíveis através dos URL`s contidos no certificado da TSU. Se a verificação é efetuada após o período de validade do correspondente certificado, consultar secção 7.2, da DPVC (disponível em https://pki.multicert.com/index.html), para orientação.

1.3 Limites de Confiança

A hora indicada no selo temporal emitido pela EVC da MULTICERT tem uma precisão (em relação ao UTC) máxima de 10ms, sendo garantido no mínimo uma precisão de 100ms. Os registos (*logs*) da EVC da MULTICERT são guardados durante 20 anos, estando durante esse tempo disponíveis como evidência de suporte à precisão da hora indicada nos selos temporais.

A plataforma tecnológica dos serviços de validação cronológica está configurada de acordo com os seguintes indicadores e métricas:

- Disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização.

1.4 Obrigações dos Subscritores/Titulares

É obrigação dos subscritores dos selos temporais:

a) Limitar e adequar a utilização dos selos temporais de acordo com a legislação vigente e com o presente documento,

b) Efetuar o pedido de emissão de selos temporais de acordo com o RFC 3161 [13],

c) Aquando da receção do selo temporal pedido, verificar que o selo temporal foi corretamente assinado pela EVC da MULTICERT,

d) Aquando da receção do selo temporal pedido, verificar que a chave privada utilizada para assinar o selo temporal é válida (i.e., não foi comprometida),

e) Não monitorizar, manipular ou efetuar ações de “engenharia inversa” sobre a implantação técnica (*hardware* e *software*) dos serviços de certificação, sem a devida autorização prévia, por escrito, da MULTICERT TS CA.

1.5 Obrigações de Verificação do Estado do Certificado pelas *Relying Parties*

É obrigação das partes que confiem nos selos temporais emitidos pela EVC da MULTICERT:

a) Limitar a fiabilidade dos selos temporais às utilizações permitidas para os mesmos, em conformidade com a legislação vigente e aplicável, e com o presente documento.

b) Verificar que o selo temporal foi corretamente assinado.

c) Verificar que a chave privada utilizada para assinar o selo temporal não foi comprometida até ao momento da verificação.

d) Verificar o estado dos selos temporais, de acordo com a secção 6.2.6 da Declaração de Práticas de Validação Cronológia.

e) Assumir a responsabilidade pela correta verificação dos selos temporais;

f) Notificar qualquer acontecimento ou situação anómala relativa ao selo temporal, utilizando os meios que a Multicert publique na sua Declaração de Práticas de Certificação (MULTICERT_PJ:ECRAIZ_427) disponível em https://pki.multicert.com.

1.6 Limites de Responsabilidade

A TSA da Multicert recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas na DPVC.

A Limitações às obrigações da TSA são as seguintes:

a) Responde pelos atos e omissões no exercício da sua atividade de acordo com o Artº 15 do DL 12/2021;

b) Assume toda a responsabilidade mediante terceiros pelas funções necessárias à prestação de serviços de confiança;

c) A responsabilidade da administração / gestão assenta sobre base objetivas e abrange todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;

d) Só responde pelos danos e prejuízos causados pelo uso indevido do selo temporal, quando não tenha consignado no selo temporal, de forma clara reconhecida por terceiros o limite quanto ao possível uso;

e) Não responde quando o Subscritor superar os limites que figuram neste documento quanto às possíveis utilizações do selo temporal;

f) Não responde se a parte confiante dos selos temporais não cumprir com as suas obrigações;

g) Não assume qualquer responsabilidade no caso de perda ou prejuízo:

   i. Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;

   ii. Ocasionados pelo uso dos selos temporais quando excedam os limites de utilização estabelecidos neste documento;

   iii. Ocasionado pelo uso indevido ou fraudulento dos selos temporais emitidos pela TSA da Multicert.

1.7 Acordos e Declaração de Práticas Aplicáveis

É aplicável o disposto na Declaração de Práticas de Validação Cronológica (MULTICERT_PJ.CA3_24.1.1_0002_pt), e Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) no que respeita aos requisitos referidos na DPVC, disponíveis em https://pki.multicert.com.

1.8 Política de Privacidade

A Multicert tem implementadas medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação Portuguesa e Europeia.

A Política de Privacidade encontra-se disponível em https://www.multicert.com/pt/termos-de-utilizacao-e-politicas/.

1.9 Indemnizações

De acordo com a legislação em vigor.

1.10 Legislação Aplicável e Disposições para Resolução de Conflitos

Em caso de litígio o consumidor pode recorrer a uma Entidade de Resolução Alternativa de Litígios de consumo. A Lista oficial de tais Entidades está disponível no Portal do Consumidor em www.consumidor.pt.

Sem prejuízo da possibilidade de recurso prévio à mediação, caso não seja obtido acordo entre as partes no âmbito de tal procedimento quanto a qualquer conflito decorrente da interpretação, aplicação ou execução do presente documento, qualquer uma das partes poderá recorrer à via judicial, ficando desde já fixado como foro competente para o efeito a Comarca de Lisboa.

1.11 Auditoria

A Multicert assegura o cumprimento das leis e normas aplicáveis, sendo realizadas auditorias anuais por uma entidade independente (CAB) para verificação do seu cumprimento, de acordo com a secção 8 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

Em particular, a TSA da Multicert está em conformidade com:

a) Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014;
b) Decreto-Lei nº 12/2021;
c) ETSI EN 319 401;
d) ETSI EN 319 421;
e) ETSI EN 319 422.

Aprovação

Nuno Ponte (Grupo de Trabalho de Gestão)

[Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte

Digitally signed by [Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte
Date: 2022.04.08 17:13:15 +01'00'