DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

POLÍTICA E PRÁTICAS DE CERTIFICAÇÃO
DE
VALIDAÇÃO CRONOLÓGICA

VERSÃO 2.3 – 01/08/2024
[IDIOMA: PORTUGUÊS]

HISTÓRICO DE VERSÕES

Data	*Edição n.º*	*Conteúdo*
10/04/2013	1.0	Redação Inicial
21/12/2017	1.1	Revisão
27/01/2021	2.0	Revisão e publicação após criação das ACs
18/05/2022	2.1	Revisão
27/04/2023	2.2	Revisão
01/08/2024	2.3	Revisão

DOCUMENTOS RELACIONADOS

Document Details	*Author(s)*
Declaração de Práticas de Certificação	DigitalSign

AUTORIZAÇÕES

Elaborado por	*Aprovado por*
	

AVISO LEGAL

Copyright © DigitalSign - Certificadora Digital, SA. Todos os direitos reservados.
DigitalSign é uma marca registada da DigitalSign – Certificadora Digital, SA. Todas as restantes marcas, trademarks e service marks são propriedade dos seus respetivos detentores.

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido a suporte@digitalsign.pt.

CONTEÚDO

1. INTRODUÇÃO

O objetivo deste documento é definir a política, as práticas e procedimentos utilizados no suporte às atividades de Validação Cronológica pela Entidade Certificadora da DigitalSign – Certificadora Digital, SA ("EC DIGITALSIGN").

Este documento está conforme a Internet Engineering Task Force (IETF) RFC 3628 para Políticas e Práticas de Certificação de Validação Cronológica, podendo sofrer atualizações regulares.

1.1. CONTEXTUALIZAÇÃO

O serviço de Validação Cronológica da EC DIGITALSIGN utiliza a infraestrutura de chaves públicas e fontes de tempo confiáveis para disponibilizar selos temporais fiáveis e conforme padrões globalmente aceites.

Este documento (Política e Práticas de Certificação de Validação Cronológica) define as práticas e políticas utilizadas para a operação e gestão do serviço de validação cronológica da EC DIGITALSIGN, de forma a que os subscritores e as partes confiantes possam avaliar o nível de confiança da operação deste serviço.

O objetivo do serviço de validação cronológica é o de disponibilizar selos temporais usados como suporte às assinaturas eletrónicas qualificadas, conforme Regulamento 910/2014 do Parlamento Europeu e do Conselho, de 23 de Julho, e demais legislação nacional aplicável.

Não obstante, os selos temporais podem também ser utilizados para qualquer outro objetivo que requeira prova que determinado(s) dado(s) existiu(ram) numa determinada data/hora.

As práticas de criação, assinatura e emissão de certificados, assim como a revogação de certificados inválidos levadas a cabo por uma Entidade de Certificação ("EC") são fundamentais para garantir a fiabilidade e confiança de uma Infraestrutura de Chaves Públicas ("PKI").

Este documento respeita e implementa os seguintes standards:

- ETSI TS 102.023: *Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*
- RFC 3628: *Requirements for Time-Stamping Authorities*

Esta Política e Práticas de Certificação de Validação Cronológica e seguintes correções e/ou atualizações, são aprovadas pelo Grupo de Gestão (ver 9.17.1. da DPC).

As correções e/ou atualizações deverão ser publicadas sob a forma de novas versões deste documento, substituindo qualquer versão anterior.

1.2. DESIGNAÇÃO E IDENTIFICAÇÃO DO DOCUMENTO

Este documento é a Política e Práticas de Certificação de Validação Cronológica da EC DIGITALSIGN, devendo ser lida em conjunto com a versão corrente da Declaração de Práticas de Certificação (DPC) da EC DIGITALSIGN, disponível para consulta em: https://pki.digitalsign.pt. Não foi associado nenhum identificador a este documento.

Este documento é identificado pela seguinte informação:

Informação do Documento	
Versão/Edição	2.3
Data de Aprovação	01/08/2024
Data de Validade	Não aplicável
Localização	https://pki.digitalsign.pt

2. REFERÊNCIAS

- ETSI TS 101.456: *Policy Requirements for Certification Authorities Issuing Qualified Certificates*
- ETSI TS 101.861: *Time-stamping Profile*
- ETSI TS 102.023: *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities*
- ETSI TS 102.176.1: *Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms*
- CPS: *Declaração de Práticas de Certificação da EC DIGITALSIGN*
- RFC 3161: *Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)*

3. ACRÓNIMOS E DEFINIÇÕES

EC	Entidade Certificadora
EC DIGITALSIGN	Entidade Certificadora da DigitalSign – Certificadora Digital, SA
DPC	Declaração de Práticas de Certificação
PKI	Infraestrutura de Chaves Públicas
OID	Número único de "identificador de objeto"
LCR	Lista de Certificados Revogados
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
UTC	Coordinated Universal Time
EVC	Entidade de Validação Cronológica (*Time Stamp Authority*)

4. CONCEITOS GERAIS

4.1. SERVIÇOS DE VALIDAÇÃO CRONOLÓGICA

Os serviços de validação cronológica incluem os seguintes componentes:

- Componentes técnicos que emitem os selos temporais;
- Componentes de gestão, controlo e monitorização do serviço de validação cronológica, incluindo a sincronização com fontes de tempo UTC confiáveis.

4.2. ENTIDADE DE VALIDAÇÃO CRONOLÓGICA

A Entidade de Validação Cronológica (EVC) é confiável pelos seus utilizadores (i.e., subscritores e partes confiantes) para emissão de selos temporais seguros. A EVC da EC DIGITALSIGN é responsável pela operação de um ou mais serviços de validação cronológica identificados na secção 4.1 anterior.

4.3. SUBSCRITORES

Os subscritores são os utilizadores finais dos selos temporais emitidos pela EVC da EC DIGITALSIGN.

Os subscritores podem ser indivíduos ou organizações (públicas ou privadas), assim como equipamentos tecnológicos.

4.4. POLÍTICA E PRÁTICAS DE CERTIFICAÇÃO DE VALIDAÇÃO CRONOLÓGICA

Este documento deve ser lido em conjunto com a versão corrente da Declaração de Práticas de Certificação (DPC) da EC DIGITALSIGN, disponível para consulta em: https://pki.digitalsign.pt, a qual regula a operação da EC DIGITALSIGN e seus serviços de certificação digital.

4.4.1. OBJETIVO

Este documento especifica a política e as práticas de certificação do serviço de validação cronológica da EC DIGITALSIGN, de forma a satisfazer os requisitos de segurança e confiabilidade descritos na secção 2 deste documento.

Para detalhes adicionais, ver a seção 7.1 deste documento.

4.4.2. NÍVEL DE ESPECIFICIDADE

Este documento descreve em geral as regras de emissão e gestão de selos temporais. A descrição detalhada do sistema é compilada em documentos adicionais de acesso restrito, apenas disponíveis a pessoal autorizado e auditores.

4.4.3. ABORDAGEM

Esta política foi trabalhada ao nível geral, não descrevendo qualquer detalhe técnico sobre o sistema informático e de comunicações, a estrutura da organização e os procedimentos de operação e de proteção. Esta política não define o ambiente computacional em que este serviço está a funcionar.

Os detalhes técnicos e de operação podem ser consultados na Declaração de Práticas de Certificação (DPC) da EC DIGITALSIGN descrita acima.

5. POLÍTICA DE SELOS TEMPORAIS

5.1. CONTEXTUALIZAÇÃO

Esta Política de Selos Temporais define um conjunto de processos para a criação de selos temporais, de acordo com a norma ETSI TS 102.023.

A EVC assina eletronicamente os selos temporais utilizando chaves privadas que são reservadas especificamente para esse efeito. As chaves privadas de assinatura de selos temporais são armazenadas em dispositivo criptográfico (HSM) dedicado e homologado.

Cada selo temporal contém um identificador de política e é emitido com uma precisão mínima de 1 (um) segundo em relação ao UTC.

Os selos temporais são pedidos através do protocolo *Transmission Control Protocol* (TCP) ou *Hypertext Transfer Protocol* (HTTP), conforme especificado no RFC 3161.

5.2. IDENTIFICAÇÃO

Hierarquia	OID de Política de Selos Temporais
RSA	1.3.6.1.4.1.25596.2.1.1
ECDSA	1.3.6.1.4.1.25596.2.1.2

O identificador é referenciado em todos os selos temporais emitidos pela EVC da EC DIGITALSIGN, e esta política está disponível a todos os subscritores e partes confiantes.

5.3. COMUNIDADE DE UTILIZADORES E APLICABILIDADE

A comunidade de utilizadores para os serviços de validação cronológica da EC DIGITALSIGN inclui os subscritores e as partes confiantes. Todos os subscritores são automaticamente considerados partes confiantes.

A EC DIGITALSIGN pode disponibilizar serviços públicos de validação cronológica.

A EC DIGITALSIGN não impõe restrições de aplicabilidade dos selos temporais, com as exceções dos casos previstos na sua DPC.

5.4. CONFORMIDADE

A EC DIGITALSIGN referencia o identificador de política na secção 5.2 (*Identificação*) deste documento em todos os selos temporais emitidos, de forma a indicar a conformidade com esta política.

A EC DIGITALSIGN é sujeita a auditorias independentes externas e internas, de forma a demonstrar que o serviço de validação cronológica cumpre as obrigações definidas na seção 6.1 (*Obrigações da EVC*) e tem implementados os controlos apropriados conforme descrito na secção 7 (*Requisitos sobre as Práticas da EVC*).

6. RESPONSABILIDADES E OBRIGAÇÕES

Este capítulo descreve as obrigações, responsabilidades e garantias da EVC, dos subscritores e das partes confiantes.

6.1. OBRIGAÇÕES DA EVC

6.1.1. OBRIGAÇÕES GERAIS

A EC DIGITALSIGN opera a EVC e assume a responsabilidade dos requisites descritos na secção 7 (*Requisitos sobre as Práticas da EVC*) deste documento, assim como o disposto em legislação nacional e europeia aplicável.

Estas obrigações e responsabilidades são reguladas por acordos mútuos assinados entre as partes, onde a Política e Práticas de Certificação de Validação Cronológica (este documento) e a Declaração de Práticas de Certificação (CPS) são partes integrantes.

6.1.2. OBRIGAÇÕES DA EVC PERANTE OS SUBSCRITORES

A DigitalSign assume as seguintes obrigações perante os subscritores do serviço d validação cronológica:

- A sua atividade de validação cronológica baseia-se em equipamento e software credenciado.
- Opera em conformidade com o disposto na Política e Práticas de Certificação de Validação Cronológica (este documento) e a Declaração de Práticas de Certificação (CPS), assim como outras políticas e procedimentos relevantes.
- Assegura que os selos temporais mantêm uma precisão mínima de 1 (um) segundo em relação ao UTC.
- Submete-se a auditorias e avaliações internas e externas para garantir a conformidade com a legislação pertinente e com as políticas e procedimentos adotados.
- Proporciona um acesso de alta disponibilidade aos sistemas de obtenção de selos temporais, exceto em casos de interrupções técnicas programadas, perda de sincronia de tempo e outros casos descritos na secção 9.8 (*Limitações de Responsabilidade da EC*) da DPC.

6.2. OBRIGAÇÕES DOS SUBSCRITORES

Os subscritores têm de garantir que os selos temporais foram corretamente assinados, assim como verificar a LCR a fim de confirmar que a chave privada utilizada para a assinatura desses selos temporais não se encontra comprometida.

Os subscritores têm de usar o padrão RFC 3161 para a solicitação de selos temporais.

6.3. OBRIGAÇÕES DAS PARTES CONFIANTES

Antes de confiar num selo temporal, as partes confiantes têm de verificar que o mesmo foi corretamente assinado, assim como verificar a LCR a fim de confirmar que a chave privada utilizada para a assinatura desse selo temporal não foi comprometida.

A parte confiante deverá ter em consideração eventuais limitações de utilização dos selos temporais indicados neste documento, assim como as precauções previstas neste documento e outros referenciados.

Durante o período de validade do certificado de validação cronológica, o estado da sua chave privada poderá ser verificado através da consulta da LCR. Caso a verificação do selo temporal seja efetuada após o período de validade do certificado, as partes confiantes deverão proceder de acordo com o disposto no Anexo D da norma ETSI TS 102.023.

6.4. RESPONSABILIDADE FINANCEIRA

A DigitalSign compromete-se a operar o serviço de validação cronológica de acordo com esta Política e Práticas de Certificação de Validação Cronológica e a Declaração de Práticas de Certificação (CPS), bem como com os acordos estabelecidos entre as partes.

A DigitalSign não assume qualquer responsabilidade expressa ou implícita nem garante (exceto em casos de acordos estabelecidos) a disponibilidade ou precisão do serviço de validação cronológica.

7. REQUISITOS SOBRE AS PRÁTICAS DA EVC

A disponibilização de selos temporais, em resposta a um pedido de emissão, fica ao critério da DigitalSign e depende de acordo com o subscritor.

7.1. DECLARAÇÕES DE PRÁTICAS E DIVULGAÇÃO

7.1.1. DECLARAÇÃO DE PRÁTICAS DA EVC

Esta Política e Práticas de Certificação de Validação Cronológica estabelece as regras gerais relativas à operação da EVC.

A DPC e demais documentos internos definem como a DigitalSign satisfaz os requisitos técnicos, organizacionais e processuais identificados nesta Política e Práticas de Certificação de Validação Cronológica.

Os documentos públicos, incluindo este documento e a DPC, podem ser consultados através do repositório da DigitalSign em: https://pki.digitalsign.pt. Os documentos internos apenas poderão ser fornecidos sobre condições estritamente controladas.

A EC DIGITALSIGN realiza avaliações de risco para determinar ameaças e definir os controlos de segurança e procedimentos operacionais necessários.

7.1.2. DECLARAÇÃO DE DIVULGAÇÃO DA EVC

Esta Política e Práticas de Certificação de Validação Cronológica, em conjunto com a DPC, são os documentos disponíveis publicamente conforme descrito no ponto 7.1.1 deste documento.

Este documento divulga a todos os subscritores e partes confiantes os termos e condições de utilização dos serviços de validação cronológica da DigitalSign. Uma síntese dos elementos da Declaração de Divulgação da EVC estão abaixo:

- O serviço de validação cronológica é operado pela EC DIGITALSIGN, e está devidamente credenciado junto da Autoridade Nacional de Segurança, conforme legalmente estipulado.
- Os dados de contacto estão referidos na secção 1.5.2 da DPC.
- Cada um dos selos temporais emitidos pela EC DIGITALSIGN contém um identificador de política, conforme descrito na secção 5.2 deste documento.
- Os algoritmos criptográficos e tamanho de chaves utilizados estão em conformidade com a norma ETSI TS 101.861, e são correntemente:
  - Algoritmos de *hash* aceites nos pedidos: SHA1, SHA256, SHA384, SHA512
  - Algoritmos de assinatura: sha256WithRSAEncryption (2048 bit key)
- A DigitalSign não estabelece outros limites de confiança para além dos dispostos na secção 6.3 anterior. A DigitalSign informará, pelos meios apropriados, os subscritores e as partes confiantes no caso dos algoritmos criptográficos e/ou os tamanhos de chave utilizados já não serem considerados seguros.
- As obrigações dos subscritores estão descritas na secção 6.2 deste documento.
- As obrigações das partes confiantes estão descritas na secção 6.3 deste documento.
- A DigitalSign mantém arquivo de registos relacionados com a operação do serviço de validação cronológica de acordo com o disposto na seção 5.5 da DPC

- A DigitalSign poderá cobrar taxas pelo serviço de validação cronológica.

7.2. GESTÃO DE CICLO DE VIDA DAS CHAVES

Esta Política e Práticas de Certificação de Validação Cronológica, em conjunto com a DPC, são os documentos disponíveis publicamente conforme descrito no ponto 7.1.1 deste documento.

7.2.1. GERAÇÃO DA CHAVE

A DigitalSign gera as chaves criptográficas utilizadas para a assinatura de selos temporais em dispositivo HSM credenciado segundo a norma FIPS 140-2 Nível 3, por pessoal autorizado, num ambiente físico seguro.

Os algoritmos e o tamanho de chave utilizados estão descritos na secção 7.1.2 deste documento.

7.2.2. PROTEÇÃO DA CHAVE

A DigitalSign adotou medidas específicas para assegurar que as chaves privadas utilizadas para a assinatura de selos temporais permanecem confidenciais e mantêm a sua integridade. Estas medidas incluem a utilização de HSMs credenciados segundo a norma FIPS 140-2 Nível 3 ou superior.

Quando são feitas cópias de segurança a essas chaves, esse procedimento é efetuado por pessoal autorizado, requerendo pelo menos a custódia dupla, e em ambiente físico seguro. Qualquer cópia de segurança é sempre efetuada para arquivo cifrado ou diretamente para outro equipamento criptográfico (HSM).

7.2.3. DISTRIBUIÇÃO DA CHAVE

Os certificados digitais usados pelo serviço de validação cronológica são emitidos pela EC DIGITALSIGN, respeitando as práticas, políticas e procedimentos descritos na DPC, providenciando um nível de segurança equivalente a esta política de validação cronológica.

Informação adicional poderá ser encontrada na secção 6.1.4 da DPC.

7.2.4. RENOVAÇÃO DA CHAVE

A DigitalSign requer que para o efeito seja criado um novo par de chaves, para substituir o par de chaves expirante (tecnicamente definido como «re-key», mas neste documento identificado como «renovação»).

As chaves são renovadas antes do termo do seu período de validade.

7.2.5. DESTRUIÇÃO DA CHAVE

As chaves usadas pelo serviço de validação cronológica são substituídas após a sua expiração. Não são emitidos selos temporais com recurso a chaves expiradas. Após a sua expiração, as chaves privadas são destruídas.

7.2.6. GESTÃO DO CICLO DE VIDA DO MÓDULO CRIPTOGRÁFICO

A DigitalSign adotou medidas específicas para assegurar que os módulos criptográficos (HSMs) utilizados nos serviços de não-repudiação não são violados no transporte ou armazenamento.

Todos os HSMs são reinicializados antes da sua utilização, por pessoal autorizado e em ambiente físico seguro.

Sempre que um HSM é submetido a intervenção técnica ou é desativado, todas as chaves armazenadas não apagadas (*zeroisation*), de cordo com as instruções do fabricante.

7.3. VALIDAÇÃO CRONOLÓGICA

7.3.1. SELOS TEMPORAIS

De acordo com os protocolos referenciados na secção 2 deste documento, cada selo temporal inclui, mas não limitado a:

- Uma representação (valor de *hash*) dos dados que são validados cronologicamente, conforme informação do subscritor;
- Um número de série único;
- Um identificador de política de validação cronológica;
- O valor tempo;
- Uma assinatura eletrónica qualificada gerada com recurso à chave criptográfica privada de uso exclusivo do serviço de validação cronológica.

7.3.2. SINCRONIZAÇÃO DO RELÓGIO

A hora utilizada é definida a partir do tempo universal coordenado (UTC) e certificada pelo instituto nacional de medida (Observatório Astronómico de Lisboa), com incerteza inferior a 100 milissegundos (ms).

Os relógios de todos os sistemas de processamento de informação da DigitalSign estão sincronizados com uma fonte de tempo precisa interna e do Observatório Astronómico de Lisboa, que mantêm a Hora Legal Portuguesa.

7.4. GESTÃO E OPERAÇÃO DA EVC

7.4.1. GESTÃO DE SEGURANÇA

Todos os assuntos relacionados com a gestão da segurança são referidos na secção 5.2 da DPC.

7.4.2. AVALIAÇÃO DE RISCOS

De forma a assegurar que todos os ativos de informação são sujeitos a um apropriado tratamento de segurança, a DigitalSign mantem um inventário de ativos, com as correspondentes classificações de risco, de forma a efetuar uma análise de risco consistente.

7.4.3. SEGURANÇA DE PESSOAL

Todos os assuntos relacionados com a gestão da segurança de pessoal são referidos na secção 5.3 da DPC.

7.4.4. SEGURANÇA FÍSICA

Todos os assuntos relacionados com a gestão da segurança de pessoal são referidos na secção 5.1 da DPC.

7.4.5. GESTÃO DE OPERAÇÕES

A EC DIGITALSIGN implementa um conjunto extenso de controlos em conformidade com a norma ETSI TS 102.023, que fazem parte de documentação interna.

A EC DIGITALSIGN é sujeita a auditorias independentes externas e internas, de forma a demonstrar que o serviço de validação cronológica cumpre todas as obrigações definidas.

Informação adicional sobre a gestão de operações pode ser encontrada na secção 5 da DPC.

7.4.6. GESTÃO DE ACESSOS AOS SISTEMAS

Os assuntos relacionados com a gestão de acessos aos sistemas são referidos nas secções 5 e 6 da DPC.

7.4.7. AMBIENTE DE CONFIANÇA

Os assuntos relacionados com o ambiente de confiança são referidos na secção 6 da DPC.

7.4.8. COMPROMETIMENTO DOS SERVIÇOS DE VALIDAÇÃO CRONOLÓGICA

Em caso de comprometimento da chave criptográfica privada utilizada no serviço de validação cronológica, a DigitalSign seguirá os procedimentos descritos na secção 5.7 da DPC. Tal inclui a revogação do respetivo certificado digital e a sua inclusão na LCR.

Em caso de perda de sincronização de relógio, e que tal implique a perda da precisão assumida, a DigitalSign interrompe a emissão de selos temporais até que a calibração esteja novamente dentro dos parâmetros definidos. Na eventualidade de se detetar a emissão de selos temporais com uma precisão que não cumpra o especificado na secção 7.3.2, a DigitalSign utilizará todos os esforços comercialmente razoáveis para notificar os subscritores e as partes confiantes afetadas.

7.4.9. EXTINÇÃO DA EVC

Em caso de extinção da EVC, a DigitalSign seguirá os procedimentos descritos na secção 5.8 da DPC. Tal inclui, pelo menos, a informação aos subscritores, a revogação dos certificados digitais utilizados no serviço de validação cronológica e a transição dos serviços para uma EC sucessora, garantindo que a entidade a quem é transmitida toda a documentação se obriga à sua manutenção durante o período de tempo legalmente exigido.

7.4.10. REQUISITOS LEGAIS

A DigitalSign atua de acordo com as normas portuguesas e europeias aplicáveis, assim como no escrupuloso cumprimento do disposto no capítulo 7.4.10 da norma ETSI TS 102.023.

7.4.11. REGISTOS DE AUDITORIA

O sistema utilizado pela DigitalSign no serviço de validação cronológica incorpora ferramentas de recolha e tratamento de registos de auditoria.

7.5. ORGÂNICA

A estrutura organizacional, políticas, procedimentos e controlos da EC DIGITALSIGN são aplicados ao serviço de validação cronológica.