

Declaração de Divulgação de Princípios de Validação Cronológica

Políticas

PJ.CC_24.1.13_0002_pt

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: Cartão de Cidadão

Nível de Acesso: Público

Versão: 5.0

Data: 26/08/2020

Identificador do documento: PJ.CC_24.1.13_0002_pt

Palavras-chave: CC, Cartão de Cidadão, SVC, Time-Stamping, Declaração de Divulgação de Princípios de Validação Cronológica

Tipologia documental: Políticas

Título: Declaração de Divulgação de Princípios de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 26/08/2020

Periodicidade de Revisão: 2 anos

Versão atual: 5.0

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: Cartão de Cidadão

Cliente: Ministério da Justiça

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
0.1	09/12/2013	Versão inicial.	MULTICERT S.A.
1.0	25/03/2014	Versão Aprovada	Grupo de Gestão
1.1	24/10/2016	Inclusão de referências inerentes ao regulamento 910/2014	GT Políticas
1.2	30/05/2017	Revisão	INCM
1.3	23/11/2017	- Revisão do valor atribuído à precisão de hora do selo temporal emitido pela EVC - Outras revisões	GT Políticas/IRN/AMA/INCM
2.0	06/12/2017	Versão Aprovada	Grupo de Gestão
2.1	23/02/2018	- Atualização das referências da EC emissora do certificado da EVC que passou a ser a EC de Assinatura Digital Qualificada do Cartão de Cidadão - Outras revisões	GT Políticas
3.0	23/02/2018	Versão Aprovada	Grupo de Gestão
3.1	09/03/2018	Inclusão de medidas tomadas em caso de não cumprimento da utilização normal do serviço	INCM/IRN
4.0	09/03/2018	Versão Aprovada	Grupo de Gestão
4.1	06/05/2020	Revisão - atualização das referências bibliográficas	INCM/IRN
5.0	26/08/2020	Versão aprovada	Grupo de Gestão

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CC_24.1.1_0002_pt_AsC.pdf	Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão	MULTICERT S.A.
PJ.CC_24.1.2_0007_pt_root.pdf	Política de Certificado de Validação Cronológica	MULTICERT S.A.
PJ.CC_24.1.1_0005_pt_root.pdf	Declaração de Práticas de Validação Cronológica	MULTICERT S.A.

Resumo Executivo

Decorrente da implementação de vários programas públicos e privados para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação, do governo eletrónico (*eGovernment*) e do comércio eletrónico (*eCommerce*), os selos temporais (*time-stamps*) emitidos pela Entidade de Certificação do Cartão de Cidadão, fornecem os mecanismos necessários para comprovar que um *datum* (conjunto de informação em formato eletrónico) existia na data da aposição do selo temporal.

A Entidade de Validação Cronológica do Cartão de Cidadão está devidamente credenciada pela Autoridade Nacional de Segurança (<https://www.gns.gov.pt/trusted-lists.aspx>), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de selos temporais, incluindo os selos temporais emitidas por Entidades de Certificação que emitem certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação). A sua infraestrutura tecnológica fornece selos temporais e mecanismos de validação cronológica, de acordo com o *standard* ETSI TS 102 023, alterado pelo ETSI EN 319 421.

A Declaração de Divulgação de Princípios de Validação Cronológica não constitui a totalidade da Declaração de Práticas sob a qual se rege a emissão de selos temporais (*time-stamps*) pela Entidade de Certificação do Cartão de Cidadão. Para este efeito deve ser consultada a Declaração de Práticas de Validação Cronológica disponível em http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.I.1_0005_pt.pdf.

Sumário

Declaração de Divulgação de Princípios de Validação Cronológica	1
Resumo Executivo	3
Sumário	4
Introdução	5
Objetivos	5
Público-Alvo	5
Estrutura do Documento.....	5
I Declaração de Divulgação de Princípios	6
I.1 Informação de contacto	6
I.2 Tipo de Selo Temporal e sua utilização	6
I.3 Limites de confiança	7
I.4 Obrigação dos subscritores	7
I.5 Obrigação das partes confiantes	7
I.6 Limites de responsabilidade	8
I.7 Acordos e Declaração de Práticas aplicável	8
I.8 Proteção de dados pessoais	8
I.9 Indemnizações.....	9
I.10 Legislação aplicável e Disposições para resolução de conflitos	9
I.11 Auditoria	9
Referências Bibliográficas	10
Validação.....	11

Introdução

Objetivos

Este documento pretende resumir, de forma simples e acessível, as características descritas na Declaração de Práticas de Validação Cronológica da Entidade de Certificação do Cartão de Cidadão (EC do Cartão de Cidadão), no suporte à sua atividade de emissão de selos temporais e fornecimento de mecanismos de validação cronológica.

Público-Alvo

Este documento deve ser lido por:

- Subscritores do serviço de Validação Cronológica da EC do Cartão Cidadão,
- Todo o público, em geral.

Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública, assinatura eletrónica e selo temporal. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimentos nos tópicos anteriormente focados, antes de proceder com a leitura do documento.

I Declaração de Divulgação de Princípios

Nesta secção, a Entidade de Validação Cronológica do Cartão de Cidadão (EVC) divulga a todos os seus subscritores e potenciais partes confiantes, os termos e condições da utilização dos serviços de validação cronológica, numa linguagem acessível e fácil compreensão.

Esta secção não deverá ser vista como um resumo de todas as práticas e políticas seguidas pela EVC, mas como um resumo de alguns dos pontos mais importantes, pelo que a leitura desta secção deve ser complementada com a leitura da Declaração de Práticas de Validação Cronológica – DPVC – (disponível em http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.I.1_0005_pt.pdf).

I.1 Informação de contacto

Entidade	MINISTÉRIO DA JUSTIÇA
Morada	IRN I.P. Av. D. João II, n° 1.8.01D Edifício H Campus da Justiça Apartado 8295 1803-001 Lisboa
Correio eletrónico	cartaodecidadao@irn.mj.pt
Telefone	211 950 500

I.2 Tipo de Selo Temporal e sua utilização

A EVC do Cartão de Cidadão emite selos temporais qualificados, de acordo com as regras e requisitos do Regulamento (EU) N° 910/2014 para validade de longo prazo, mas é aplicável a qualquer uso, que tenha uma exigência de qualidade equivalente.

O selo temporal emitido pela EVC do Cartão de Cidadão inclui o OID da política de Validação Cronológica, garantido aos subscritores e partes confiantes, a conformidade com essa política. As representações, garantias, limitações e obrigações dos vários participantes na Validação Cronológica estão descritas nas secções 9.6, 9.7 e 9.8 da DPVC - Declaração de Práticas de Validação Cronológica (disponível em http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.I.1_0005_pt.pdf)

A EVC do Cartão de Cidadão aceita pedidos de selo temporal dos seus subscritores, de acordo com o RFC 3161. O algoritmo de *hash* utilizado para representar o *datum* ao qual se vai apor o selo temporal é o SHA-256.

O acesso a este serviço não requer autenticação, mas existem limites temporais e de quantidade no acesso ao serviço, de forma a manter o nível de serviço e evitar utilizações abusivas. O serviço está por

isso limitado a um máximo de 20 pedidos em cada período de 20 minutos. Se este valor for excedido o serviço será bloqueado durante 24 horas, sem prejuízo de outras consequências em caso de repetição de situações de bloqueio. Caso se verifiquem comportamentos abusivos que evidenciem o não cumprimento da utilização normal do serviço, revelando consumos anormais, o serviço será bloqueado e registado em lista negra, impossibilitando a utilização do mesmo a partir da origem (IP público) na qual se verificou o referido comportamento abusivo.

Qualquer selo temporal é assinado digitalmente pela TSU da EVC do Cartão de Cidadão, por um certificado digital com um mínimo de seis 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. Se a verificação for efetuada após o período de validade do correspondente certificado, consultar secção 7.2, da DPVC (disponível em http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.I.1_0005_pt.pdf), para orientação.

1.3 Limites de confiança

A hora indicada no selo temporal emitido pela EVC do Cartão de Cidadão tem uma precisão que (em relação ao UTC) garante uma precisão de +/- 1s ou melhor, relativamente a esta referência.

Os dados sujeitos a arquivo são retidos pelo período de tempo de 7 anos, após a expiração do certificado que assinou o selo temporal, 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 99,990%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização.

1.4 Obrigação dos subscritores

É obrigação dos subscritores dos selos temporais:

- Limitar e adequar a utilização dos selos temporais de acordo com as normas/legislação aplicáveis, o presente documento e com as práticas descritas na Declaração de Validação Cronológica (http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.I.1_0005_pt.pdf),
- Efetuar o pedido de emissão de selos temporais de acordo com o RFC 3161,
- Aquando da receção do selo temporal pedido, verificar que o selo temporal foi corretamente assinado pela EVC do Cartão de Cidadão,
- 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),
- 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 EC do Cartão de Cidadão.

1.5 Obrigação das partes confiantes

É obrigação das partes que confiem nos selos temporais emitidos pela EVC do Cartão de Cidadão:

- Limitar a fiabilidade dos selos temporais às utilizações permitidas para as mesmas em conformidade com as normas/legislação aplicáveis 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 comprometida¹,
- d) Assumir a responsabilidade na correta verificação dos selos temporais,
- e) Notificar qualquer acontecimento ou situação anómala relativa ao selo temporal, utilizando os sítios Web do Instituto dos Registos e Notariado e do <https://eportugal.gov.pt/>.

1.6 Limites de responsabilidade

A EVC do Cartão de Cidadão recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas na DPVC.

A Limitações às obrigações são as seguintes:

- a) A responsabilidade da administração / gestão da EVC do Cartão de Cidadão assenta sobre base objetivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços
- b) A EVC do Cartão de Cidadão não responde quando o subscritor superar os limites que figuram neste documento quanto às possíveis utilizações do selo temporal.
- c) A EVC do Cartão de Cidadão não responde se a parte confiante dos selos eletrónicas não cumprir com as suas obrigações,
- d) A EVC do Cartão de Cidadão não assume qualquer responsabilidade no caso de perda ou prejuízo:
 - ii) Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior,
 - iii) Ocasionalmente pelo uso dos selos temporais quando excedam os limites de utilização estabelecidos neste documento,
 - iv) Ocasionalmente pelo uso indevido ou fraudulento dos selos temporais emitidos pela EVC do Cartão de Cidadão.

1.7 Acordos e Declaração de Práticas aplicável

É aplicável o disposto na Declaração de Práticas de Validação Cronológica – DPVC – (disponível em http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.I.1_0005_pt.pdf).

1.8 Proteção de dados pessoais

No âmbito da Entidade de Validação Cronológica e na utilização de selos temporais, apenas é considerado dado pessoal o IP a partir do qual é efetuado o pedido, ficando este registado nos sistemas da EVC.

Este dado pessoal não é alvo de tratamento, apenas é retido durante o tempo definido por lei, para efeitos de registos de auditoria.

¹ Note-se que 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. Se a verificação é efetuada após o fim do período de validade do correspondente certificado, consultar secção 7.2 da DPVC - Declaração de Práticas de Validação Cronológica (disponível em http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.I.1_0005_pt.pdf) para orientação.

I.9 Indemnizações

Nada a assinalar.

I.10 Legislação aplicável e Disposições para resolução de conflitos

Todas as reclamações entre subscritores e EVC do Cartão de Cidadão deverão ser comunicadas pela parte em disputa à Entidade Supervisora, com o fim de tentar resolvê-lo entre as mesmas partes.

Para a resolução de qualquer conflito que possa surgir com relação a esta DDPVC, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à Jurisdição de Contencioso Administrativo.

A conformidade exigida remete-se para o regulamento (EU) 910/2014 e *standards* aplicáveis, referidos na secção das Referências Bibliográficas deste documento.

I.11 Auditoria

As auditorias de conformidade são realizadas regularmente com os *standards* aplicáveis. A EC demonstra, com a auditoria e Relatório de Conformidade (produzidos por um Organismo de Avaliação da Conformidade), que a avaliação dos riscos foi assegurada, tendo sido identificadas e implementadas todas as medidas necessárias para a segurança de informação.

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional, com o descrito na secção 8 da DPVC - Declaração de Práticas de Validação Cronológica (disponível em http://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.1.1_0005_pt.pdf), e outras regras, procedimentos e processos.

Referências Bibliográficas

CWA 14167-1: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements*, Junho de 2003.

ETSI TS 101 733. 2013-04, *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)*, v2.2.1.

ETSI TS 102 176-1. 2011-07, *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms*, v2.1.1

ETSI TS 102 023, 2008-10. *Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*, v1.2.2. alterado pelo ETSI EN 319 421 (2016), *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*

ETSI EN 319 422 v1.1.1, 2016. *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles*.

ETSI EN 319 401 v2.2.1, 2018. *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*.

CA/Browser Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*

Regulamento (EU) N° 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para transações eletrónicas no mercado interno e que revoga a *Diretiva 1999/93/CE*

ITU-R Recommendation TF.460-5. 1997, *Standard-frequency and time-signal emissions*.

ITU-R Recommendation TF.536-1. 1998, *Time scale notations*.

RFC 3161. 2001, *Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)*.

RFC 3628. 2003, *Policy Requirements for Time-Stamping Authorities (TSAs)*.

Lei 41/2004 (alterada e republicada pela lei 46/2012) - Regula a proteção de dados pessoais no sector das Comunicações Eletrónicas

Regulamento Geral de Proteção de Dados - <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>

Lei 58/2019 Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Validação