Declaração de Divulgação de Princípios da Entidade de Validação Cronológica do Cartão de Cidadão

Políticas (POL#32)

Nível de Acesso: Público

Versão: 6.0

Data: Mar 2024

IRN – Instituto dos Registos e Notariado, I.P.
Av. D. João II, Lote 1.08.01, Edifício H, Parque das Nações 1990-097 Lisboa, Portugal
Telefone: +351 217 985 500 e-mail: geral@irn.mj.pt

Identificador do Documento: POL#32

Palavras-chave: PKI CC, Cartão de Cidadão, Entidade de Validação Cronológica, Divulgação de Princípios

Tipologia Documental: Políticas

Título: Declaração de Divulgação de Princípios da Entidade de Validação Cronológica do Cartão de Cidadão

Nível de acesso: Público

Autor: IRN - Instituto dos Registos e Notariado, I.P.

Data: Mar 2024

Versão atual: 6.0

Validade do Documento: 2 (dois) anos após a sua aprovação.

Histórico de Versões

Versão	Data	Detalhes
1.0	25/03/2014	Versão inicial.
2.0	06/12/2017	Revisão do valor atribuído à precisão de hora do selo temporal emitido pela EVC.
3.0	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.
4.0	09/03/2018	Inclusão de medidas tomadas em caso de não cumprimento da utilização normal do serviço.
5.0	18/12/2020	Revisão do documento.
6.0	**Março 2024**	**Revisão Documental**

Documentos Relacionados

Documento	**Autor**	**Descrição**
Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão (POL#31)	IRN	Descreve os procedimentos e práticas utilizados pela Entidade de Validação Cronológica do Cartão de Cidadão para suportar a sua atividade de emissão de selos temporais qualificados.
Política de selo temporal qualificado (POL#26)	IRN	Descreve a Política de selo temporal qualificado, de acordo com os requisitos gerais para serviços de confiança de emissão de selos temporais.
Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão (POL#23)	IRN	Descreve a Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.

Estado do documento

Este é um documento controlado e aprovado pelo IRN.

Embora este documento possa ser impresso, a versão eletrónica assinada digitalmente pelo(s) elemento(s) do Grupo de Gestão, é a cópia controlada. Qualquer cópia impressa deste documento não é controlada.

Sendo um documento **controlado** e de **acesso público**, este documento pode ser arquivado em unidades locais ou de rede, assim como ser acedido diretamente no repositório da PKI do Cartão de Cidadão em https://pki.cartaodecidadao.pt/.

Índice

1 Introdução

Este documento resume (mas não substitui), de forma simples e acessível, as características descritas na "Política de selo temporal qualificado" e na "Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão" (disponíveis em https://pki.cartaodecidadao.pt/). É elaborado tendo em conta as especificações técnicas indicadas no anexo B da norma ETSI EN 319 421[1].

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 Validação Cronológica 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 infraestrutura da Entidade de Certificação do Cartão de Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promove a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Validação Cronológica do Cartão de Cidadão (EVC do Cartão de Cidadão) está credenciada pela Autoridade Nacional de Segurança (https://www.gns.gov.pt/trusted-lists.aspx), conforme Regulamento (UE) n.º 910/2014[2] (Regulamento eIDAS), estando deste modo habilitada legalmente a emitir selos temporais qualificados, que beneficiam da presunção da exatidão da data e da hora que indicam e da integridade dos dados aos quais a data e a hora estão associadas. A infraestrutura tecnológica da EVC do Cartão de Cidadão fornece selos temporais e mecanismos de validação cronológica, de acordo com o IETF RFC 3161[3] e os standards ETSI EN 319 421[1] e ETSI EN 319 422[4].

A Declaração de Divulgação de Princípios da Entidade de Validação Cronológica do Cartão de Cidadão não constitui uma Política sob a qual se regem os selos temporais emitidos pela mesma. Para este efeito devem ser consultadas a "Política de selo temporal qualificado" e a "Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão", disponíveis em https://pki.cartaodecidadao.pt/.

1.1 Público-Alvo

Este documento deve ser lido por:

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

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 conhecimento nos tópicos anteriormente focado antes de proceder com a leitura do documento.

[1] ETSI EN 319 421, *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*
[2] 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.
[3] *cf.* IETF RFC 3161. 2001, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*.
[4] ETSI EN 319 422, *Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles*

2 Contactos da Entidade de Validação Cronológica do Cartão de Cidadão

O contacto principal da Entidade de Validação Cronológica do Cartão de Cidadão é o seguinte:

Nome	**IRN I.P. - Departamento de Identificação Civil** **MINISTÉRIO DA JUSTIÇA**
Morada	Av. D. João II, nº 1.8.01D, Edifício H Campus da Justiça Apartado 8295 1803-001 Lisboa
Correio eletrónico	cartaodecidadao@irn.mj.pt
Telefone	211 950 500

3 Tipos de selos temporais, procedimentos de validação e utilização

O selo temporal emitido pela EVC do Cartão de Cidadão é denominado de **selo temporal qualificado**, já que o serviço de emissão de selo temporal prestado pelo IRN[5] (prestador qualificado de serviços de confiança) se encontra credenciado de acordo com o Regulamento (UE) nº 910/2014[2] (cf. https://www.gns.gov.pt/trusted-lists.aspx).

O selo temporal qualificado emitido pela EVC do Cartão de Cidadão:

- É assinado por um certificado de selo eletrónico de validação cronológica (certificado VC, cf. POL#23[6]);
- Inclui o identificador (OID) de política 0.4.0.2023.1.1 (BTSP - *best practices policy for time-stamp* -, definido no ETSI EN 319 421[1]), declarando a sua conformidade com essa política de selo temporal, e de modo a permitir que partes confiantes e outras pessoas interessadas possam saber qual a política de selo temporal seguida;
- O algoritmo de *hash* utilizado para representar o *datum* ao qual se vai apor o selo temporal é o SHA-256;
- É assinado digitalmente pela TSU da EVC do Cartão de Cidadão por um certificado digital com um mínimo de seis anos de validade;
- Está conforme com o perfil e características descritas na "Política de selo temporal qualificado" (POL#26).

3.1 Utilização do selo temporal

A EVC do Cartão de Cidadão está disponível em http://ts.cartaodecidadao.pt/tsa/server, estando o formato de pedido e de resposta de selo temporal, de acordo com os formatos indicados no ETSI EN 319 422[4] e IETF RFC 3161[3]. Responde a pedidos de selos temporais efetuados pelos subscritores:

- Pessoas individuais, sem autenticação, limitado a um máximo de 20 pedidos de selos temporais em cada período de 20 minutos (se o valor for excedido, o serviço será bloqueado durante 24 horas);
- Pessoas individuais ou pessoas coletivas, com autenticação, sem limite de pedidos. Estes são casos excecionais, que têm de ser analisados e aprovados pelo Grupo de Gestão.

Os selos temporais qualificados emitidos pela EVC do Cartão de Cidadão podem ser utilizados sempre que é necessário vincular dados em formato eletrónico a uma hora específica, criando uma prova de que esses dados existiam nesse momento. Em particular, podem ser utilizados para validade a longo prazo de documentos, por exemplo conforme definido na norma ETSI EN 319 122-1[7] (ou noutras normas com requisitos equivalentes).

Os serviços de validação cronológica oferecidos pela EVC do Cartão de Cidadão não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram uma atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, 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.

[5] IRN - Instituto dos Registos e Notariado, I.P.
[6] POL#23 Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão.
[7] ETSI EN 319 122-1 *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*

As representações, garantias, limitações e obrigações dos vários participantes na Validação Cronológica estão descritas nas secções 10.6, 10.7 e 10.8 da DPVC – "Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão" (disponível em https://pki.cartaodecidadao.pt/)

3.2 Validação do selo temporal

Uma aplicação ou uma parte confiante deve validar o seguinte, ao processar o selo temporal qualificado, de modo a avaliar se confia no mesmo:

- Verificar que o selo temporal qualificado foi corretamente assinado;
- Verificar que a chave privada utilizada para assinar o selo temporal qualificado, não foi comprometida;
- A extensão "*policy*" do selo temporal indica o OID da política que rege a emissão de selos temporais.

A aceitação do selo temporal é da responsabilidade exclusiva da parte confiante ou da aplicação que o processa,

4 Limites de confiança

A hora indicada no selo temporal emitido pela EVC do Cartão de Cidadão está sincronizado com duas fontes de tempo indicadas pelo *Bureau International des Poids et Mesures* (BIPM), garantindo-se uma precisão de +/- 1s ou melhor.

Os dados sujeitos a arquivo são retidos pelo período legal, estando durante esse tempo disponíveis como evidência de suporte à precisão da hora indicada nos selos temporais.

5 Obrigação dos subscritores

É obrigação dos subscritores dos selos temporais:

a) Limitar e adequar a utilização dos selos temporais de acordo com a legislação vigente, o presente documento e com as práticas descritas na DPVC (disponível em https://pki.cartaodecidadao.pt/),

b) Efetuar o pedido de emissão de selos temporais de acordo com o IETF RFC 3161[3],

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

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 EVC do Cartão de Cidadão.

6 Obrigação das partes confiantes

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

a) Limitar a fiabilidade dos selos temporais às utilizações permitidas para as mesmas em conformidade com as normas/legislação aplicáveis e com o expresso no presente documento, na Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão, e na Política de selo temporal correspondente,

b) Verificar que o selo temporal foi corretamente assinado,

c) Verificar que a chave privada utilizada para assinar o selo temporal não foi comprometida[8],

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 Portal do Cidadão.

A aceitação do selo temporal é da responsabilidade exclusiva da parte confiante ou da aplicação que o processa,

[8] 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 8.2 da DPVC (disponível em https://pki.cartaodecidadao.pt/) para orientação.

7 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.

As 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 eletrónicos não cumprir com as suas obrigações,

d) A EVC do Cartão de Cidadão não assume qualquer responsabilidade no caso de perca 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 emitidas pela EVC do Cartão de Cidadão.

8 Acordos e Declaração de Práticas aplicável

É aplicável o disposto na:

- "Política de selo temporal qualificado",
- "Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão" (DPVC).

Estes documentos encontram-se disponíveis em https://pki.cartaodecidadao.pt/.

9 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 do Cartão de Cidadão.

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

10 Indemnizações

De acordo com a legislação em vigor.

11 Legislação aplicável e Disposições para resolução de conflitos

É aplicável à atividade inerente da EVC do Cartão de Cidadão a legislação nacional, o Regulamento (EU) nº 910/2014[2] e standards internacionais indicados nas Referências Bibliográficas deste documento.

11.1 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.

Sem prejuízo da possibilidade de recurso prévio à mediação, caso não seja obtido acordo entre as partes no âmbito de tal procedimento, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à Jurisdição de Contencioso Administrativo.

12 Auditoria

Todas as intervenções realizadas à Entidade de Validação Cronológica do Cartão de Cidadão são devidamente auditadas por auditores internos. A EVC do Cartão de Cidadão é auditada por um Organismo de Avaliação da Conformidade (devidamente registado no Organismo Nacional de Acreditação), o qual emite um Relatório de Conformidade (CAR[9]) que é disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança, conforme regulamento eIDAS[2] (conforme âmbito descrito na secção 9 da DPVC , disponível em https://pki.cartaodecidadao.pt/).

12.1 Certificações

O prestador qualificado de serviço de confiança (IRN - Instituto dos Registos e Notariado, I.P.) está certificado para a emissão de selo temporal qualificado, conforme regulamento eIDAS[2], podendo tal ser verificado na *eIDAS Trusted List* em eIDAS Dashboard (europa.eu).

[9] *Conformity Assessment Report*

Referências Bibliográficas

- ETSI EN 319 421, *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*.
- ETSI EN 319 422, *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles*.
- ETSI EN 319 401, *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*.
- Regulamento (EU) Nº 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.
- Decreto-Lei nº 12/2021, de 9 de fevereiro, que assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.
- IETF RFC 3161. 2001, *Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP*).
- Lei 41/2004 - Regula a proteção de dados pessoais no sector das Comunicações Eletrónicas
- Regulamento Geral de Proteção de Dados - Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho da União Europeia, 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 e que revoga a Diretiva 95/46/CE.
- Lei n.º 58/2019 de 8 de agosto: 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.

Aprovação

Aprovado pelo Grupo de Gestão.

Assinado por: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2024.03.04 19:48:03+00'00'