

Declaração de Divulgação de Princípios de Validação Cronológica

Políticas

PJ.CC_24.1.13_0002_pt_root

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: Cartão de Cidadão

Nível de Acesso: Público

Versão: 1.0

Data: 25/03/2014

Identificador do documento: PJ.CC_24.1.13_0002_pt_root

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: 25/03/2014

Versão atual: 1.0

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 |

Documentos Relacionados

| ID Documento | Detalhes | Autor(es) |
|-------------------------------|---|----------------|
| PJ.CC_24.1.1_0001_pt_root.pdf | Declaração de Práticas de Certificação 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, os selos temporais (*time-stamps*) emitidos pelo serviço de Validação Cronológica da Entidade de Certificação do Cartão de Cidadão, credenciada pela Autoridade Credenciadora (conforme previsto na legislação europeia e nacional), 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 fornece selos temporais e mecanismos de validação cronológica, de acordo com a legislação nacional e europeia, conforme com o *standard* ETSI TS 102 023 [4].

A Entidade de Certificação do Cartão de Cidadão está devidamente credenciada pela Autoridade Nacional de Segurança (<http://www.gns.gov.pt/assinatura-electronica.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).

Este documento foi elaborado tendo em conta as especificações técnicas relatadas no anexo B da norma “*ETSI TS 102 023: Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*” [4].

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 <https://pki.cartaodecidadao.com/politicas/dpvc.html>.

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 contato | 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 | 7 |
| I.7 Acordos e Declaração de Práticas aplicável | 8 |
| I.8 Privacidade dos dados pessoais..... | 8 |
| I.9 Indemnizações..... | 8 |
| I.10 Legislação aplicável e Disposições para resolução de conflitos | 8 |
| I.11 Auditoria | 9 |
| Referências Bibliográficas | 10 |

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.

A Entidade de Certificação do Cartão de Cidadão está devidamente credenciada pela Autoridade Nacional de Segurança (<http://www.gns.gov.pt/assinatura-electronica.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).

Público-Alvo

Este documento deve ser lido por:

- Clientes 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 conhecimento nos tópicos anteriormente focado 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 <https://pki.cartaodecidadao.pt/publico/politicas/cps.html>).

I.1 Informação de contato

| NOME | Grupo de Políticas da EC do Cartão de Cidadão |
|---------------------|---|
| Morada: | IRN I.P. – DCC Av. D. João II, nº 1.8.01D Edifício H Campus da Justiça Apartado 8295 1803-001 Lisboa |
| Correio eletrónico: | cartaodecidadao@dgrn.mj.pt |
| Telefone: | +351 707 200 886 |

I.2 Tipo de Selo Temporal e sua utilização

A EVC do Cartão de Cidadão emite selos temporais qualificadas de acordo com as regras e requisitos da Directiva 1999/93/CE [9] para validade de longo prazo (como definido na TS 101 733 [2]), 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 adequada, 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 <https://pki.cartaodecidadao.pt/publico/politicas/cps.html>)

A EVC do Cartão de Cidadão aceita pedidos de selo temporal dos seus subscritores, 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.

Qualquer selo temporal é assinado digitalmente pela TSU da EVC do Cartão de Cidadão, por um certificado digital com um 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. Se a verificação é efetuada após o período de validade do correspondente certificado, consultar secção 7.2, da DPVC (disponível em <https://pki.cartaodecidadao.pt/publico/politicas/cps.html>), para orientação.

I.3 Limites de confiança

A hora indicada no selo temporal emitido pela EVC do Cartão de Cidadão tem uma precisão (em relação ao UTC) máxima de 10ms, sendo garantido no mínimo uma precisão de 100ms. Os registos (*logs*) da EVC do Cartão de Cidadão 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.

I.4 Obrigação dos subscritores

É obrigação dos subscritores dos selos temporais:

- limitar e adequar a utilização dos selos temporais de acordo com a legislação vigente e com o presente documento,
- efetuar o pedido de emissão de selos temporais de acordo com o RFC 3161 [13],
- aquando da receção do selo temporal pedido, verificar que o selo temporal foi corretamente assinada 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.

I.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 a legislação vigente e com o presente documento,
- verificar que o selo temporal foi corretamente assinada,
- verificar que a chave privada utilizada para assinar o selo temporal não foi comprometida¹,
- assumir a responsabilidade na correta verificação dos selos temporais,
- notificar qualquer acontecimento ou situação anómala relativa ao selo temporal, utilizando os meios que a EC do Cartão de Cidadão publique no seu sítio Web.

I.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:

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 da TSU. 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 <https://pki.cartaodecidadao.pt/publico/politicas/cps.html>) para orientação.

- a) a EVC do Cartão de Cidadão responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Artº 26 do DL 62/2003 [7].
- b) a EVC do Cartão de Cidadão assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação.
- c) 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
- d) a EVC do Cartão de Cidadão 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) 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.
- f) a EVC do Cartão de Cidadão não responde se a parte confiante dos selos eletrónicas não cumprir com as suas obrigações,
- g) 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) ocasionados pelo uso dos selos temporais quando excedam os limites de utilização estabelecidos neste documento,
 - iv) ocasionado pelo uso indevido ou fraudulento dos selos temporais emitidas 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 <https://pki.cartaodecidadao.pt/publico/politicas/cps.html>).

1.8 Privacidade dos dados pessoais

O Ciclo de Vida, é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa.

É considerada informação privada toda a informação fornecida pelo subscritor, que não seja disponibilizada no selo temporal.

A responsabilidade de proteção da informação privada segue o disposto na Legislação portuguesa.

1.9 Indemnizações

De acordo com a legislação em vigor.

1.10 Legislação aplicável e Disposições para resolução de conflitos

Todas reclamações entre utilizadores e EVC do Cartão de Cidadão deverão ser comunicadas pela parte em disputa à Autoridade Credenciadora, 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.

É aplicável à atividade das entidades certificadoras e entidades de validação cronológica a seguinte legislação específica:

- a) Despacho n° 27008/2004, de 14 de Dezembro, publicado no D.R II, n° 302, de 28 de Dezembro;
- b) Portaria n° 1350/2004, de 23 de Outubro;
- c) Despacho n° 16445/2004, de 29 de Julho, publicado no D.R II, n° 190 de 13 de Agosto;
- d) Aviso n° 8134/2004, de 29 de Julho, publicado no D.R II, n° 190 de 13 de Agosto;
- e) Decreto Regulamentar n°. 25/2004, de 15 de Julho [8];
- f) Decreto-Lei n° 290-D/99, de 2 de Agosto [6] com as alterações introduzidas pelo Decreto-Lei n° 62/2003, de 3 de Abril [7] e Decreto-lei n° 165/2004, de 6 de Julho;

Portaria n° 1370/2000, publicada no D.R. n° 21 I, II série de 12 de Setembro.

É responsabilidade da Autoridade Credenciadora zelar pelo cumprimento da legislação aplicável.

1.1 Auditoria

As auditorias de conformidade são realizadas regularmente de acordo com a legislação². A EC precisa de provar, com a auditoria e relatório de segurança anuais (produzidos pelo auditor de segurança acreditado), que a avaliação dos riscos foi assegurada, tendo sido identificado e implementado 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 <https://pki.cartaodecidadao.pt/publico/politicas/cps.html>), e outras regras, procedimentos e processos.

² cf. Decreto Regulamentar n.º 25/2004, de 15 de Julho.

Referências Bibliográficas

- [1] CWA 14167-1: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements*, Junho de 2003.
- [2] ETSI TS 101 733. 2008-07, *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CADES)*, v1.7.4.
- [3] ETSI TS 101 861. 2006-01, *Time stamping profile*, v1.3.1.
- [4] ETSI TS 102 023. 2008-10, *Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*, v1.2.2.
- [5] ETSI TS 102 176-1. 2007-11, *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms*, v2.0.0
- [6] *Decreto-Lei n.º 290-D/99*, de 2 de Agosto.
- [7] *Portaria n.º 1370/2000*, publicada no D.R. n.º 211, II série de 12 de Setembro.
- [8] *Decreto-Lei n.º 62/2003*, de 3 de Abril.
- [9] *Decreto Regulamentar n.º 25/2004*, de 15 de Julho.
- [10] *Portaria n.º 1350/2004*, de 23 de Outubro;
- [11] *Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas electrónicas*, Jornal Oficial n.º L 013 de 19/01/2000 p. 0012 – 0020.
- [12] ITU-R Recommendation TF.460-5. 1997, *Standard-frequency and time-signal emissions*.
- [13] ITU-R Recommendation TF.536-1. 1998, *Time scale notations*.
- [14] *Portaria n.º 701-G/2008*, de 29 de Julho, I Série.
- [15] RFC 3161. 2001, *Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)*.
- [16] RFC 3628. 2003, *Policy Requirements for Time-Stamping Authorities (TSAs)*.

Validação