CARTÃO DE CIDADÃO

Política de selo temporal qualificado

Políticas (POL#26)

Nível de Acesso: Público

Versão: 2.0

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#26

Palavras-chave: PKI CC, Cartão de Cidadão, Política, Selo Temporal

Tipologia Documental: Políticas

Título: Política de selo temporal qualificado

Nível de acesso: Público

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

Data: Mar 2024

Versão atual: 2.0

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

Histórico de Versões

Versão	Data	Detalhes
1.0	Nov 2022	Versão inicial.
2.0	**Mar 2024**	**Revisão Documental**

Documentos Relacionados

Documento	Autor	Descrição
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

Decorrente da implementação de vários programas públicos 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 e do governo eletrónico (e*Government*), os selos temporais (*time-stamps*), emitidos pela Entidade de Validação Cronológica (*Time-Stamping Authority*) do Cartão de Cidadão, fornecem os mecanismos necessários para vincular dados em formato eletrónico a uma hora específica, criando uma prova de que esses dados existiam nesse momento.

A Entidade de Validação Cronológica do Cartão de Cidadão (EVC CC) está credenciada pela entidade supervisora (Autoridade Nacional de Segurança) para a emissão de selos temporais qualificados, de acordo com o Regulamento (UE) nº 910/2014[1] (cf. https://www.gns.gov.pt/trusted-lists.aspx).

Este documento (Política de selo temporal qualificado) descreve a política de selo temporal que está conforme os requisitos para serviços de confiança de emissão de selos temporais, identificados no ETSI EN 319 421[2].

1.1 Público-Alvo

O público-alvo deste documento são as entidades que utilizam os serviços da EVC CC para a emissão de selos temporais, assim como as terceiras partes de confiança,

Assume-se que o leitor deste documento é conhecedor dos conceitos de criptografia e selos temporais. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nesses tópicos antes de prosseguir com a leitura do documento.

Este documento complementa a "Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão"[3], presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

[1] Regulamento (UE) 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 as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.
[2] ETSI EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*
[3] Documento identificado pelo OID 2.16.620.1.1.1.2.4.4.0.7, disponível no repositório da PKI do Cartão de Cidadão, em https://pki.cartaodecidadao.pt/ .

2 Contexto Geral

O presente documento é um documento que tem como objetivo a descrição de um conjunto de parâmetros e requisitos do selo temporal, emitido pela Entidade de Validação Cronológica do Cartão de Cidadão (EVC CC). Não se pretende nomear regras legais ou obrigações, mas antes informar pelo que se pretende que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

O selo temporal emitido pela EVC CC é denominado de **selo temporal qualificado**, já que o serviço de emissão de selo temporal prestado pelo IRN[4] (prestador qualificado de serviços de confiança) se encontra credenciado de acordo com o Regulamento (UE) nº 910/2014[1] (cf. https://www.gns.gov.pt/trusted-lists.aspx).

O selo temporal qualificado emitido pela EVC CC:

- É assinado por um certificado de selo eletrónico de validação cronológica (certificado VC, cf. POL#23[5]);
- 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[2]), 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.

A EVC CC 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[6] e RFC 3161[7].

2.1 Visão Geral

Este documento satisfaz e complementa os requisitos impostos pela "Declaração de Práticas da Entidade de Validação Cronológica do Cartão de Cidadão"[3], e está conforme a política BTSP (*best practices policy for time-stamp* -, definido no ETSI EN 319 421[2]), pela qual a emissão de selos temporais da EVC CC se rege.

2.2 Designação e Identificação do Documento

Este documento é a "Política de selo temporal qualificado", sendo identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Nome	Política de selo temporal qualificado
Versão	2.0
Estado	Aprovado
OID	2.16.620.1.1.1.2.4.4.0.1.1
Data	Mar 2024

[4] IRN - Instituto dos Registos e Notariado, I.P.
[5] POL#23 Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão.
[6] ETSI EN 319 422 *Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles*
[7] IETF RFC 3161 *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*

INFORMAÇÃO DO DOCUMENTO	
Validade	Até 2 (dois) anos após a sua aprovação, ou até que seja substituído por uma nova versão (o que ocorrer primeiro)
Localização	https://pki.cartaodecidadao.pt/

3 Política

Esta política está de acordo com a política BTSP (*best practices policy for time-stamp*) definida no documento ETSI EN 319 421[2].

3.1 Geral

A política de selo temporal pela qual a EVC CC se rege é a política BTSP (- *best practices policy for time-stamp* -, definido no ETSI EN 319 421[2]). A política BTSP é uma política que contempla as melhores práticas para Entidades de Validação Cronológica que emitem selos temporais, com base em certificados de selo eletrónico, com uma precisão melhor ou igual a um segundo.

3.2 Identificação

A política BTSP é identificada pelo OID 0.4.0.2023.1.1, que corresponde a:

> *itu-t*(0) *identified-organization*(4) *etsi*(0) *time-stamp-policy*(2023) *policy-identifiers*(1) *best-practices-ts-policy*(1)

3.3 Utilização

Esta política aplica-se aos selos temporais qualificados emitidos pela EVC CC. A EVC CC responde a pedidos de selos temporais efetuados por:

- 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.

3.4 Aplicabilidade

Os selos temporais qualificados emitidos pela EVC CC 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[8] (ou noutras normas com requisitos equivalentes).

3.5 Perfil do selo temporal

O perfil do selo temporal está em conformidade com o ETSI EN 319 422[6] e RFC 3161[7], e contém os campos e extensões indicadas na secção 3.5.8.

[8] ETSI EN 319 122-1 *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*

3.5.1 Número da Versão

O campo "*version*" do selo temporal descreve a versão utilizada na codificação do mesmo, sendo utilizado o valor 1.

3.5.2 OID da Política

O campo "*policy*" do selo temporal indica o OID da política pela qual se rege a emissão de selos temporais. No caso do selo temporal qualificado emitido pela EVC CC, o OID é o 0.4.0.2023.1.1 (cf. secção 3.2).

3.5.3 Data e Hora

O campo "*genTime*" do selo temporal indica a data e hora em que foi gerado o selo temporal qualificado pela EVC CC. Esta data e hora é sincronizada com fontes de tempo confiável, garantindo rastreabilidade para o tempo UTC[9](k) através de um dos laboratórios UTC(k) identificados pelo BIPM (*Bureau International des Poids et Mesures*) na sua Circular T (https://www.bipm.org/en/bipm-services/timescales/time-ftp/Circular-T.html).

3.5.4 Precisão

O campo "*accuracy*" do selo temporal identifica a precisão do "*genTime*" (cf. secção 3.5.3) a que o selo temporal qualificado foi criado. A precisão tem de ser melhor ou igual a um segundo – caso a EVC CC não consiga fornecer essa precisão, o selo temporal não é emitido –.

3.5.5 Dados vinculados

O campo "*messageImprint*" do selo temporal contém a *hash* (com algoritmo identificado por "*hashAlgorithm*") dos dados aos quais o "*genTime*" está vinculado, ou seja, contém a *hash* dos dados que o selo temporal vai comprovar que existiam no momento "*genTime*".

Esses dados do campo "*messageImprint*" contêm a *hash* dos dados e o "*hashAlgorithm*" indicado no pedido de selo temporal, pelo cliente da EVC CC (cf. secção 3.3).

A EVC CC aceita o "*hashAlgorithm*" sha256.

3.5.6 Certificado de assinatura

O selo temporal qualificado é assinado pela EVC CC, através de um certificado de selo eletrónico de validação cronológica (certificado VC, cf. POL#23[5]).

3.5.7 Semântica de processamento

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;

[9] UTC – *Coordinated Universal Time*

- 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,

3.5.8 Campos e extensões

Os campos e as extensões utilizados na resposta da EVC CC ao pedido de selo temporal estão em conformidade com o ETSI EN 319 422[6] e RFC 3161[7], sendo identificados na tabela seguinte (embora com algumas simplificações, para facilitar a compreensão da resposta).

3.5.8.1 Perfil de resposta da EVC CC

Campo	Valor	Tipo[10]	Comentários
1. StatusInfo			*Informação de estado de emissão do selo temporal*
1.1 status	< valor de acordo com secção 2.4.2 do RFC 3161[7] >	m	Se o valor for 0 ("*Granted*"), o selo temporal foi emitido e o "*TimeStampToken*" está incluído na resposta.
1.2 statusString	< descrição do "*status*" >	o	
1.3 failInfo	< valor de acordo com secção 2.4.2 do RFC 3161[7] >	o	Quando o "*TimeStampToken*" não está incluído na resposta, indica a razão de tal ter ocorrido.
2. timeStampToken		*o*	*O selo temporal, propriamente dito*
2.1 TSTInfo		m	
2.1.1 version	1	m	Versão do formato do selo temporal
2.1.2 policy	0.4.0.2023.1.1	m	OID da política pela qual se rege a emissão de selos temporais
2.1.3 messageImprint		m	Contém a *hash* dos dados e o "*hashAlgorithm*" indicado no pedido de selo temporal, pelo cliente da EVC CC.
hashAlgorithm message	2.16.840.1.101.3.4.2.1 < *hash* (com algoritmo identificado por "*hashAlgorithm*") dos dados aos quais o "*genTime*" está vinculado >		sha256
2.1.4 serialNumber	<valor aleatório, atribuído pela EVC CC a cada selo	m	

[10] A terminologia utilizada para cada um dos tipos de campo no formato X.509, significa o seguinte:
- m – obrigatório (o campo TEM que estar presente)
- o – opcional (o campo PODE estar presente)
- c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

Campo	Valor	Tipo[10]	Comentários
	temporal>		
2.1.5 genTime	< data e hora em que foi gerado o selo temporal pela EVC CC >	m	
2.1.6 accuracy	< a precisão do "*genTime*" a que o selo temporal foi criado >	m	
2.1.7 ordering	False	o	
2.1.8 nonce	< valor de "*nonce*" fornecido no pedido de selo temporal >	o	Tem de estar presente, se existir "*nonce*" no pedido de selo temporal, caso em que o valor tem de ser igual.
2.1.9 tsa	< identificação da TSA >	o	
2.1.10 extensions		o	
2.1.10.1 Qualified Certificate Statement		m	Não é uma extensão definida no RFC 5280, mas encontra-se definida no RFC 3739 e no ETSI EN 319 412-5.
id-qcs-pkixQCSyntax-v2	*id-etsi-tsts-EuQCompliance*		Conforme secção 9.1 do ETSI 319 422[6].
2.2 signingCertificate		m	
Certificate	< certificado de selo eletrónico de validação cronológica utilizado para assinar o selo temporal >		Certificado VC, cf. POL#23[5].
CertificateIssuer	< DN do *Issuer* de "*Certificate*" >		
CertificateSerial	< Número de sério de "*Certificate*" >		
2.3. *Signature Algorithm*	1.2.840.113549.1.1.1	m	rsaEncryption
2.4. *Signature Value*	<contém a assinatura digital do selo temporal efetuada pela chave privada do "*Certificate*" >	m	Ao gerar esta assinatura, a EVC CC certifica que o "*messageImprint*" existia no momento "*genTime*".

Aprovação

Assinado por: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2024.03.04 19:46:49+00'00'