CARTÃO DE CIDADÃO

Declaração de Práticas de Validação Cronológica

Políticas

PJ.CC_24.1.1_0005_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_24.1.1_0005_pt

Palavras-chave: Cartão de Cidadão, Declaração de Práticas de Validação Cronológica

Tipologia documental: Políticas

Título: Declaração de Práticas de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 26/08/2020

Periodicidade de Revisão: 1 ano

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	08/12/2013	Versão inicial.	MULTICERT S.A.
1.0	**25/03/2014**	**Versão Aprovada**	**GT de Gestão**
1.1	03/04/2017	Revisão	GT de Políticas
1.2	18/05/2017	Alteração de Validade do certificado TSA e adaptação ao novo regulamento 910/2014	GT Gestão/INCM
1.3	05/12/2017	- Inclusão obrigações das entidades externas - Inclusão de atividades de cessação de atividade - Retificação do valor de precisão de sincronismo - Revisão da secção "2.1 - Repositório"	GT de Políticas/IRN/AMA/INCM
2.0	**06/12/2017**	**Versão Aprovada**	**Grupo de Gestão**
2.1	08/02/2018	- Revisão da secção "1.4.2 – Subscritor" - Inclusão das Entidades externas e suas responsabilidades - Atualização das referências da EC emissora do certificado da EVC que passou a ser a EC de Assinatura Digital qualificada do Cartão de Cidadão	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	04/05/2020	Revisão: - Alteração do tamanho de chaves do certificado da TSU - Atualização de referências bibliográficas - Adição de limites para utilização responsável	INCM/IRN
5.0	**26/08/2020**	**Versão aprovada**	**Versão Aprovada**

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.

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 credenciada pela Autoridade Nacional de Segurança (https://www.gns.gov.pt/trusted-lists.aspx), 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). 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.

Este documento define os procedimentos e práticas utilizadas pela Entidade de Certificação do Cartão de Cidadão no suporte à sua atividade de emissão de selos temporais e fornecimento de mecanismos de validação cronológica, sendo referenciado como o documento de Declaração de Práticas de Validação Cronológica da Entidade de Certificação do Cartão de Cidadão.

Sumário

Introdução

Objetivos

O objetivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Validação Cronológica do Cartão de Cidadão (EVC 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:

- Recursos humanos atribuídos aos grupos de trabalho da EVC do Cartão de Cidadão;
- Terceiras partes, encarregues de auditar a EVC Cartão do 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 tal não se verifique, recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focados antes de proceder com a leitura deste documento.

Os primeiros sete capítulos são dedicados a descrever os procedimentos e práticas mais importantes no âmbito dos serviços de Validação Cronológica da EVC do Cartão de Cidadão. O capítulo oito descreve auditorias de conformidade e outras avaliações. O capítulo nove descreve as matérias legais.

1 Introdução

O presente documento é uma Declaração de Práticas de Validação Cronológica, ou DPVC, cujo objetivo se prende com a definição de um conjunto de práticas para a emissão de selos temporais e fornecimento de mecanismos de validação cronológica, para a garantia de fiabilidade desses mesmos selos. 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.

Este documento descreve as práticas gerais seguidas pela Entidade de Validação Cronológica do Cartão de Cidadão (EVC do Cartão de Cidadão) na emissão de selos temporais e fornecimento de mecanismos de validação cronológica, explicando o que um selo temporal fornece e significa, assim como os procedimentos que deverão ser seguidos pelas Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos selos emitidos pela EVC do Cartão de Cidadão. Este documento é passível de sofrer atualizações regulares.

Os selos emitidos pela EVC do Cartão de Cidadão contêm uma referência à DPVC de modo a permitir que Partes confiantes e outras pessoas interessadas possam encontrar informação sobre o selo e a entidade que o emitiu.

1.1 Selo Temporal

Ao criar evidências/comprovativos digitais que sejam confiáveis e passíveis de validação, torna-se necessário utilizar um método *standard* para associar a data/hora ao *datum*, de modo a que possam ser validados posteriormente. A qualidade destas evidências é baseada no processo de criação e gestão da estrutura de dados que representa os eventos (neste caso, o registo da data/hora), assim como na qualidade dos pontos mensuráveis (neste caso, o processo como o registo da data/hora é aplicado) que ancoram as evidências ao mundo real.

Adicionalmente, para verificar uma assinatura eletrónica pode ser necessário provar que a assinatura digital do *datum*, efetuada pelo titular do certificado digital, foi efetuada enquanto o certificado era válido. Esta verificação é necessária em duas circunstâncias:

1) Durante o período de validade do certificado, caso a chave privada tenha sido comprometida e, portanto, revogada por esse motivo;

2) Após o final do período de validade do certificado, uma vez que as Entidades de Certificação não revogam certificados após o final do período de validade dos mesmos.

Um modo de resolver este problema passa pela utilização do selo temporal que permite provar que um *datum* existia antes de um determinado ponto no tempo. Esta técnica permite provar que a assinatura foi gerada antes da data/hora contida na estrutura de dados que forma o selo temporal. As práticas e políticas utilizadas na emissão e validação do selo temporal são a principal razão para a elaboração do presente documento. Convém salientar que estas práticas e políticas permitem a resolução de outras necessidades.

O selo temporal é caracterizado, também, no "*ETSI Electronic Signature Format standard TS 101 733*", criado com base no "*RFC 3161 – Time-Stamp Protocol*". Estes documentos identificam os requisitos mínimos de segurança e de qualidade necessários para a garantir a validação confiável de assinaturas eletrónicas de longo prazo.

O regulamento (EU) 910/2014 do Parlamento Europeu define prestador de serviços de confiança como "uma pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como

prestador qualificado quer como prestador não qualificado de serviço de confiança". Um exemplo de um prestador de serviços de certificação é uma Entidade de Validação Cronológica (*Time-Stamping Authority*).

1.1.1 Utilização adequada

Os requisitos e regras definidos neste documento aplicam-se a todos os selos temporais emitidos pela EVC do Cartão de Cidadão.

Os selos temporais são emitidos a pedido dos subscritores e de acordo com o RFC 3161, sendo utilizadas pelas Partes Confiantes para validação da associação da data/hora ao *datum*.

O Cartão de Cidadão disponibiliza selos temporais gratuitos aos subscritores que deles necessitem.

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.

1.1.2 Utilização não autorizada

Os selos temporais apenas poderão ser utilizados na extensão do que é permitido pela legislação aplicável (secção 9.14). Não poderão ser utilizadas para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação 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.

1.2 Visão Geral

As práticas de emissão de selos temporais e fornecimento de mecanismos de validação cronológica levadas a cabo por uma Entidade de Validação Cronológica (EVC) são fundamentais para garantir a fiabilidade e confiança no selo aposto a qualquer *datum*.

Esta DPVC aplica-se especificamente à EVC do Cartão de Cidadão que respeita e implementa os *standards* apresentados nas Referências Bibliográficas.

Este documento especifica as práticas e políticas de operação e gestão da EVC do Cartão de Cidadão, de modo a que os subscritores do serviço e partes confiantes possam ter confiança na operação dos serviços de emissão de selo temporal e validação cronológica.

1.3 Designação e Identificação do Documento

Este documento é a Declaração de Práticas de Validação Cronológica do Cartão de Cidadão.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão	Versão 5.0
Estado	Aprovado
OID	2.16.620.1.1.2.100.4.1.1
Data de Emissão	Agosto de 2020
Validade	1 ano
Localização	https://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.1.1_0005_pt.pdf

1.4 Participantes na Validação Cronológica

1.4.1 Entidade de Validação Cronológica

A Entidade em que os utilizadores (i.e., subscritores e partes confiantes) dos serviços de validação cronológica confiam para a emissão de selos temporais é designada por Entidade de Validação Cronológica (EVC). A EVC tem a responsabilidade de fornecer os serviços de selo temporal, que podem ser decompostos em duas componentes (independentemente do modo como estes serviços estejam implementados):

- Emissão de selo temporal – esta componente do serviço gera os selos temporais;
- Gestão dos serviços de validação cronológica – esta componente monitoriza e controla a operação dos serviços de validação cronológica, de modo a garantir que os mesmos são fornecidos conforme especificado neste documento de práticas e políticas. Esta componente tem a responsabilidade da ativação e desativação do serviço de emissão de selo temporal – por exemplo, para garantir que o relógio, utilizado na emissão do selo temporal, está corretamente sincronizado com o tempo UTC.

A EVC tem a responsabilidade de operar uma ou mais TSU (*time-stamping unit*) que cria e assina selos temporais em nome da EVC, cada uma com a sua chave distinta de assinatura.

A EVC pode utilizar serviços de outras partes no fornecimento dos serviços de validação cronológica, sendo contudo sempre responsável por garantir o cumprimento das práticas e políticas definidas neste documento.

1.4.2 Subscritor

O subscritor é o cidadão em nome individual ou o cidadão ao qual estão associados atributos profissionais na orgânica de uma determinada entidade pública, sendo responsável pelo cumprimento das suas obrigações, conforme disposto na secção 9.6.2.

Adicionalmente, este serviço pode ser utilizado por Entidades que tenham sido formalmente autorizadas pelo Grupo de Gestão.

1.4.3 Partes Confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação de um selo temporal ao *datum*, ou seja confiam na veracidade do selo temporal.

Nesta DPVC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do selo temporal emitido pela EVC do Cartão de Cidadão.

1.4.4 Outros participantes

1.4.4.1 Entidades externas de prestação de serviços

As Entidades que prestam serviços de suporte à EVC do Cartão do Cidadão têm as suas responsabilidades/obrigações devidamente definidas nos contratos de prestação de serviços estabelecidos. São elas a Imprensa Nacional Casa da Moeda (INCM), S.A., que por sua vez subcontratou alguns dos serviços à Multicert S.A., esta última numa óptica da manutenção técnica do serviço.

Neste âmbito os serviços contratados/subcontratados são a operação, manutenção preventiva e evolutiva, bem como a monitorização do serviço da EVC.

1.4.4.2 Fonte Legal de Tempo

No caso da EVC do Cartão de Cidadão, o relógio utilizado para emitir selos temporais está sincronizado com duas fontes de tempo indicadas pelo *Bureau International des Poids et Mesures* (BIPM).

1.4.4.3 Entidade Supervisora

Entidade Supervisora é a entidade competente para a credenciação das entidades certificadoras. De uma forma geral o papel da Entidade Supervisora, exercida em Portugal pelo Gabinete Nacional de Segurança (GNS), tem como principal função supervisionar os prestadores qualificados de serviços de confiança estabelecidos no território nacional, no sentido de verificar se os prestadores e os serviços de confiança qualificados por eles prestados cumprem os requisitos estabelecidos no regulamento eIDAS.

1.5 Política de Validação Cronológica

O presente documento define a política e práticas de validação cronológica seguidas pela EVC do Cartão de Cidadão na emissão de selos temporais, baseada em certificados digitais.

A EVC do Cartão de Cidadão emite selos temporais qualificados, de acordo com as regras e requisitos do Regulamento (EU) Nº 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 adequada, garantido a subscritores e partes confiantes a conformidade com essa política.

1.6 Gestão das Políticas

1.6.1 Entidade responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do Grupo de Trabalho de Políticas da PKI do Cartão de Cidadão.

1.6.2 Contacto

Entidade	MINISTÉRIO DA JUSTIÇA
Morada	IRN I.P. - Departamento de Identificação Civil 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

1.6.3 Entidade responsável pela determinação da conformidade da DPVC relativamente à Política

O Grupo de Trabalho de Políticas determina a conformidade e aplicação interna desta DPVC (e/ou respetivas PCs), submetendo-a de seguida ao Grupo de Gestão para aprovação.

1.6.4 Procedimentos para Aprovação da DPVC

Esta política deverá ser revista conforme a periodicidade de revisão indicado no documento, ou sempre que se verifiquem alteração nas práticas da EVC que necessitem de ser refletidas neste documento.

A revisão desta DPVC (e/ou respetivas PCs) é levada a cabo pelos Grupos de Trabalhos da EVC, dando origem a novas versões, substituindo qualquer DPVC (e/ou respetivas PCs) anteriormente definida.

O Grupo de Trabalho de Políticas deverá ainda determinar quando é que as alterações na DPVC (e/ou respetivas PCs) darão origem a uma alteração nos identificadores dos objetos (OID) da DPVC (e/ou respetivas PCs).

Após a fase de validação, a DPVC (e/ou respetivas PCs) é submetida ao Grupo de Gestão, que é a entidade responsável pela aprovação e autorização de modificações neste tipo de documentos.

1.7 Definições e acrónimos

1.7.1 Acrónimos

Acrónimo	Designação
ANSI	*American National Standards Institute*
CA	*Certification Authority* (o mesmo que EC)
CRL	Lista de Revogação de Certificados
DPVC	Declaração de Práticas de Validação Cronológica
EC	Entidade de Certificação
EVC	Entidade de Validação Cronológica
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objecto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infra-estrutura de Chave Pública)
SHA	*Secure Hash Algorithm*
TSA	*Time-Stamping Authority* (o mesmo que EVC)

1.7.2 Definições

Item	Definição
Atividades de Alto Risco	Atividades 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.
Assinatura digital	Modalidade de assinatura eletrónica avançada, baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, permitindo ao titular usar a chave privada para declarar a autoria do documento eletrónico, ao qual a assinatura é aposta e concordância com o seu conteúdo e, ao destinatário, usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura eletrónica	Resultado de um processamento eletrónico de dados, suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Assinatura eletrónica avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada	Assinatura digital, ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital, baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Entidade Supervisora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado	Certificado eletrónico, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no Regulamento (EU) Nº 910/2014.
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.

Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos.
Criptografia	Estudo de princípios e técnicas que permitem transformar a informação da sua forma original para outra ilegível, de forma que possa ser conhecida apenas pelo seu destinatário
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica.
Datum	Informação em formato digital.
Dispositivo de criação de assinatura	Suporte digital ou dispositivo utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que: i) Os dados necessários à criação de uma assinatura, utilizados na sua geração, só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura, utilizados na sua geração, não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações, realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados, na sua geração, possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular, antes do processo de assinatura.
Documento eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Estampilha Temporal	Estrutura de dados que liga a representação eletrónica de um *datum* com uma data/hora particular, estabelecendo evidência de que o *datum* existia nessa data/hora.
Informação Sensível	Dados que devem ser protegidos contra acesso não-autorizado para salvaguardar a privacidade ou segurança de um indivíduo ou organização
Informação PÚBLICA	O nível PÚBLICO, ou NÃO-CLASSIFICADO, destina-se a indicar que a informação em causa foi, sob o ponto de vista de segurança, objeto de apreciação, mas considerou-se não ser necessário atribuir-lhe qualquer outro nível de classificação. Enquadra-se neste nível toda a informação titulada pela PKI do CC que possa ser do domínio público.
Informação INTERNA	Este nível de classificação deve ser aplicado à informação cuja divulgação a terceiros possa ser desfavorável para os interesses da PKI do CC. Destina-se a preservar a segurança da informação, limitando o seu acesso aos gestores e colaboradores internos da PKI do CC que, pela sua importância, não carece de classificação mais elevada.
Informação CONFIDENCIAL	Este nível de classificação deve ser aplicado à informação cujo conhecimento por pessoas não autorizadas, possa ser prejudicial para os interesses da PKI do CC. Obriga à elaboração e manutenção, por parte do dono do ativo de informação, de uma lista de pessoas que pode ter acesso à informação
Informação RESTRITA	Este nível de classificação abrange a informação cuja divulgação ou conhecimento por pessoas não autorizadas possa ter consequências graves para a INCM, em resultado de: - Fazer perigar a concretização de empreendimentos importantes da PKI do CC; - Comprometer a segurança de planos, melhoramentos científicos ou técnicos, importantes para a PKI do CC; - Revelarem procedimentos em curso relacionados com assuntos de alta importância. Obriga à elaboração e manutenção, por parte do dono do ativo de informação, de uma lista de pessoas que podem ter acesso à informação
Informação MUITO RESTRITA	O nível de classificação "MUITO RESTRITO" é limitado à informação que necessita do mais elevado grau de proteção. Deve ser aplicado unicamente à informação, cujo conhecimento ou divulgação por pessoas não autorizadas possa implicar consequências excecionalmente graves para a organização, em virtude de: - Conduzirem a situações que possam afetar as condições de defesa os altos interesses da PKI do CC ou do Estado; - Comprometerem a segurança do Estado ou a segurança de assuntos de caráter técnico ou científico de alto interesse para a PKI do CC ou para o Estado. Obriga à elaboração e manutenção, por parte do dono do ativo de informação, de uma lista de pessoas que pode ter acesso à informação
Parte confiante	Recetor de um selo temporal que confia na mesma.
Selo Temporal	O mesmo que Estampilha temporal

Sistema TSA (*TSA system*)	Composição de produtos IT e componentes, organizados de modo a suportar o fornecimento de serviços de validação cronológica.
Subscritor	Entidade que requer os serviços de uma EVC e explícita ou implicitamente concorda com os termos e condições dos mesmos.
TSU (*time-stamping unit*)	Conjunto de *hardware* e *software* que é gerido como uma unidade e tem uma única chave de assinatura de selo temporal ativa num determinado momento.
UTC (*Coordinated Universal Time*)	Escala de tempo baseada no segundo, como definido na *ITU-R Recommendation TF.460-5*.
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1*)
Validação cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

O Ministério da Justiça é responsável pelas funções de repositório da PKI e da EVC do Cartão de Cidadão, publicando, entre outras, informação relativa às práticas adotadas.

A plataforma tecnológica do repositório está configurada de acordo com os seguintes indicadores e métricas:

- Disponibilidade do repositório a pedidos do documento da DPVC de 99,990%, em período 24hx7d, excluindo manutenções necessárias e planeadas, efetuadas em horário de menor utilização;
- Número máximo anual de pedidos da DPVC: 150.000 pedidos/ano.

O acesso à informação disponibilizada pelo repositório é efetuado através do protocolo HTTPS e HTTP, estando implementado os seguintes mecanismos de segurança:

- DPVC só pode ser alterada através de processos e procedimentos bem definidos,
- A plataforma tecnológica do repositório encontra-se devidamente protegida pelas técnicas mais atuais de segurança física e lógica,
- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

2.2 Publicação de informação de validação cronológica

A EVC do Cartão de Cidadão, disponibiliza a seguinte informação pública *on-line*:

- Cópia eletrónica desta DPVC e Políticas mais atuais da EVC do Cartão de Cidadão, disponibilizada na secção Serviço de Selos Temporais, em http://pki.cartaodecidadao.pt/:
  - Declaração de Práticas de Validação Cronológica do Cartão de Cidadão:
  - Declaração de Divulgação de Princípios de Validação Cronológica.,
  - Política de Certificado de Validação Cronológica.

Adicionalmente, serão conservadas todas as versões anteriores das DPVC da EVC do Cartão de Cidadão, disponibilizando-as a quem as solicite (desde que justificado), ficando, no entanto, fora do repositório de acesso público.

2.3 Periodicidade de publicação

As atualizações a esta DPVC e/ou respetivas PC serão publicadas imediatamente após a sua aprovação pelo Grupo de Gestão, conforme disposto na secção 9.12.

2.4 Controlo de acesso aos repositórios

A informação publicada está disponível na Internet, sendo sujeita a mecanismos de controlo de acesso permitindo apenas leitura). A EVC do Cartão de Cidadão implementou medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

3 Declaração de Divulgação de Princípios

O conteúdo desta secção está descrito na Declaração de Divulgação de Princípios de Validação Cronológica, disponível em https://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.1.13_0002_pt.pdf Nesta secção, a EVC divulga a todos os seus subscritores e partes confiantes, os termos e condições da utilização dos serviços de validação cronológica, numa linguagem fácil de entender.

Esta secção não deverá ser vista como um resumo de todas as práticas e políticas seguidas pela EVC, mas como uma síntese de alguns dos pontos mais importantes, pelo que a sua leitura deve ser complementada com a leitura do restante documento.

3.1 Informação de contacto

Conforme secção 1.1. da DDPVC - Declaração de Divulgação de Princípios de Validação Cronológica.

3.2 Tipo de Selo Temporal e sua utilização

Conforme secção 1.2. da DDPVC - Declaração de Divulgação de Princípios de Validação Cronológica

3.3 Limites de confiança

Conforme secção 1.3. da DDPVC - Declaração de Divulgação de Princípios de Validação Cronológica.

3.4 Obrigação dos subscritores

Conforme secção 9.6.2.

3.5 Obrigação das partes confiantes

Conforme secção 9.6.3.

3.6 Limites de responsabilidade

Conforme secções 9.7, e 9.8.

3.7 Acordos e Declaração de Práticas aplicável

É aplicável a presente Declaração de Práticas.

3.8 Privacidade dos dados pessoais

Conforme secção 9.4.

3.9 Indemnizações

Conforme secção 9.9.

3.10 Legislação aplicável e Disposições para resolução de conflitos

Conforme secções 9.13, 9.14 e 9.15.

3.11 Auditoria

Conforme secção 8.

4 Validação Cronológica

4.1 Selo Temporal

A EVC do Cartão de Cidadão garante que os selos temporais são emitidos de forma segura e incluem a hora/data correta. Em particular:

a) O selo temporal inclui um identificador da política de validação cronológica;

b) Cada selo temporal tem um identificador único;

c) Os valores de hora/data que a TSU utiliza no selo temporal podem ser rastreados até pelo menos um valor real de tempo distribuído por um dos laboratórios identificados na secção 1.4.4.2;

d) A hora/data incluída no selo temporal está sincronizada com o tempo UTC, garantindo-se uma precisão de +/- 1s ou melhor relativamente a esta referência;

e) Se for detetado que o relógio fornecedor do tempo a incluir no selo temporal não está dentro da precisão indicada, o selo temporal não será emitido, sendo que a EVC devolverá um erro indicando que a fonte de tempo não está disponível, tal como previsto no RFC 3161;

f) O selo temporal inclui uma representação (valor *hash*) do *datum*, conforme fornecido pelo subscritor;

g) O selo temporal é assinado por uma chave privada gerada exclusivamente para esse fim (assinatura de selos temporais);

h) O selo temporal inclui:

- O identificador do país onde a EVC está estabelecida,
- O identificador da EVC,
- O identificador da unidade (TSU) que emite o selo temporal.

4.2 Sincronização do relógio

A EVC do Cartão de Cidadão garante que o(s) relógio(s) que fornece(m) a hora/data a incluir no selo temporal está(ão) sincronizado(s) com o tempo UTC, com a precisão indicada neste documento. Em particular:

a) A calibração do relógio é mantida de tal modo a que não seja expetável que o mesmo não se encontre dentro da precisão definida neste documento;

b) O relógio está protegido contra ameaças que possam resultar numa alteração, não detetada, ao relógio que tenha como resultado uma alteração à precisão definida neste documento;

c) São detetadas as situações em que o tempo indicado no selo temporal contem desvios em relação à precisão definida neste documento;

d) A sincronização do relógio é mantida quando é introduzido um segundo intercalar, de acordo com o notificado pelos laboratórios identificados na secção 1.4.4.1.

e) O relógio é sincronizado por *appliance* GPS, sendo o tempo fornecido no máximo de *stratum* 3.

4.3 Processamento do pedido de selo temporal

O processamento do pedido de selo temporal, efetuada pelo subscritor, é satisfeito de imediato pela EVC do Cartão de Cidadão, de acordo com os limites indicados na secção 3.3.

Relativamente ao serviço de emissão de selos temporais, este está configurado de acordo com os seguintes indicadores e métricas:

- Disponibilidade de pedidos de selos temporais de 99,990%, em período 24hx7d excluindo manutenções necessárias e planeadas, efetuadas em horário de menor afluência;
- Número de pedidos de selos temporais com distribuição uniforme: até 150.000 pedidos/anos;
- Número de pedidos de selos temporais em regime de pico - até 10% a mais que o regime normal;
- Tempo médio de 2 segundos para resposta a pedidos de selos temporais, com tempo máximo de 4 segundos;
- Pedidos máximos por minuto: 40 selos temporais / minuto;
- Pedidos médios por minuto: 10 selos temporais / minuto;
- Pedidos simultâneos: 20 selos temporais.

A fim de assegurar disponibilidade do serviço a todos os utilizadores, a emissão de selos temporais é sujeita e um limite de utilização responsável: é permitido o máximo de 20 pedidos em cada período de 20 minutos, para cada endereço IP subscritor. Caso este limite seja ultrapassado, a emissão será suspensa para o endereço IP subscritor, durante um período de 24 horas.

Poderão estar isentas deste limite as entidades públicas previamente autorizadas pelo Grupo de Gestão da PKI do Cartão de Cidadão.

Em caso de compromisso de operações da TSU (por exemplo, compromisso da chave de assinatura), suspeita de compromisso ou perda de calibração da TSU, esta última não emitirá selos temporais até que seja reposto o estado normal de operação.

5 Medidas de segurança física, de gestão e operacionais

A EVC do Cartão de Cidadão implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes desta DPVC. Esta secção descreve sucintamente os aspetos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de emissão de selos temporais, auditorias e arquivo. Estes são considerados críticos para garantir a confiança nos selos temporais, pois qualquer falha de segurança pode comprometer as operações da EVC.

5.1 Medidas de segurança física

5.1.1 Localização física e tipo de construção

As instalações da EVC do Cartão de Cidadão são desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas do acesso não autorizado, dano, ou interferência. A arquitetura utiliza o conceito de defesa em profundidade, ou seja, por níveis de segurança, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior, nunca sendo possível, em qualquer local das instalações, aceder ao nível de segurança (n) a partir de outro que não seja de nível (n-1).

As operações da EVC do Cartão de Cidadão são realizadas numa sala numa zona de alta segurança, inserida noutra zona também de alta segurança e, dentro de um edifício que reúne diversas condições de segurança, nomeadamente o controlo total de acessos que previne, deteta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

As duas zonas de alta segurança são áreas que obedecem às seguintes caraterísticas:

a) Paredes em alvenaria, betão ou tijolo;

b) Teto e pavimento com construção similar à das paredes;

c) Inexistência de janelas;

d) Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança acionável eletronicamente, caraterísticas corta – fogo e funcionalidade antipânico.

Adicionalmente, as seguintes condições de segurança são garantidas no ambiente da EVC do Cartão de Cidadão:

- Perímetros de segurança claramente definidos;
- Paredes, chão e teto em alvenaria, sem janelas, que impedem acessos não autorizados;
- Trancas e fechaduras anti roubo de alta segurança, nas portas de acesso ao ambiente de segurança.
- O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;

- Acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

5.1.2 Acesso físico ao local

Os sistemas da EVC do Cartão de Cidadão estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança), garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

O acesso a cada nível de segurança requer o uso de um cartão magnético ou smartcard de controlo de acesso (amarelo para o edifício, e vermelho para os outros níveis). Os acessos físicos são, automaticamente, registados e gravados em circuito fechado de TV para efeitos de auditoria.

O acesso ao cartão de identificação vermelho obriga a um duplo controlo de autenticação de acesso individual. Não é permitida a entrada e permanência em áreas de segurança, a pessoal não acompanhado, incluindo colaboradores ou visitantes não autenticados. É obrigatória a utilização do respetivo cartão de acesso, de modo visível.

O acesso à zona mais restrita de alta segurança requer controlo duplo, cada um deles utilizando dois fatores de autenticação, incluindo autenticação biométrica.

5.1.3 Energia e ar condicionado

O ambiente seguro da EVC do Cartão de Cidadão possui equipamento redundante, que garante condições de funcionamento 24 horas por dia, 7 dias por semana de:

- Alimentação de energia elétrica, garantindo o fornecimento contínuo, ininterrupto, com a potência suficiente para manter, autonomamente, a rede elétrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações elétricas que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia e geradores de eletricidade a diesel), e
- Refrigeração/ventilação/ar condicionado, que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes no ambiente. Um sensor de temperatura ativa um alerta GSM sempre que a temperatura atinge valores anormais. Este alerta GSM, consiste em telefonemas com uma mensagem previamente gravada, para os elementos da equipa de manutenção.

5.1.4 Exposição à água

As zonas de alta segurança têm instalado os mecanismos devidos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da EVC do Cartão de Cidadão.

5.1.5 Prevenção e proteção contra incêndio

O ambiente seguro da EVC do Cartão de Cidadão tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Sistemas de Deteção Automática de Incêndio, estão instalados nos vários níveis físicos de segurança,
- Equipamento de extinção de incêndios, fixo e manual, disponíveis e colocados em sítios estratégicos, de fácil acesso, permitindo a sua utilização de forma rápida e eficaz,
- Procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6 Salvaguarda de suportes de armazenamento

Todos os suportes de informação sensível são guardados em cofres e armários de segurança dentro da zona de alta segurança, assim como num ambiente distinto externo ao edifício com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho. Para além das restrições de acessos, também tem implementados mecanismos de proteção contra acidentes (e.g., causados por água ou fogo).

Quando, para efeito de arquivo de cópias de segurança, a informação sensível é transportada da zona de alta segurança para o ambiente externo, o processo é executado por menos 2 (dois) elementos do Grupo de Trabalho que têm por obrigação garantir o transporte seguro da informação até ao local de destino. A informação (ou o *token* de transporte da informação) deverá estar sempre sob controlo visual dos membros do Grupo de Trabalho.

Em situações que implique a deslocação física de *hardware* de armazenamento de dados (i.e., discos rígidos) para fora da zona de alta segurança, por motivos que não o arquivo de cópias de segurança, cada elemento do *hardware* deverá ser verificado para garantir que não contém dados sensíveis. Nestas situações, a informação tem de ser eliminada usando todos os meios necessários para o efeito (formatar o disco rígido, *reset* do *hardware* criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7 Eliminação de resíduos

Os documentos e materiais em papel que contenham informação sensível cujo ciclo de vida tenha terminado, deverão ser eliminados através de um método que não permita a sua reconstrução (ex. trituradora).

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível (através de formatação "segura" de baixo nível ou destruição física), antes dos mesmos serem eliminados. Os equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Os outros equipamentos de armazenamento (i.e., discos rígidos, *tapes*), de modo a não ser possível recuperar o seu conteúdo, serão alvo de operações de destruição do mesmo, através de formatações seguras ou destruição física dos equipamentos.

5.1.8 Instalações externas (alternativa) para recuperação de segurança

Todas as cópias de segurança são guardadas em instalações distintas daquelas que albergam os sistemas que deram origem às referidas cópias, ficando alojadas em ambiente seguro, tais como cofres e armários seguros, situados em zonas com controlo de acesso físicos restringindo o acesso apenas a pessoal autorizado, garantindo também a proteção contra danos acidentais (e.g., causados por água ou fogo).

5.2 Medida de segurança dos processos

A atividade de uma Entidade de Validação Cronológica depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque,

- Em virtude dos requisitos de segurança inerentes ao funcionamento de uma EVC é vital garantir uma adequada segregação de funções que minimize a importância individual de cada um dos intervenientes;
- É necessário garantir que a EVC apenas poderá ser sujeita a ataques do tipo *denial-of-service* mediante o conluio de um número significativo de intervenientes.

Pelo exposto, nesta secção, descrevem-se os requisitos necessários para reconhecer os papéis de confiança e responsabilidades associadas a cada um desses papéis. Esta secção inclui também a separação de deveres, em termos dos papéis que não podem ser executados pelos mesmos indivíduos.

5.2.1 Grupos de Trabalho

Conforme secção 5.2.1 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.2.2 Número de pessoas exigidas por tarefa

Conforme secção 5.2.2 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.2.3 Funções que requerem separação de responsabilidades

Conforme secção 5.2.3 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3 Medidas de Segurança de Pessoal

Conforme secção 5.3 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Conforme secção 5.3.1 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.2 Procedimento de verificação de antecedentes

Conforme secção 5.3.2 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.3 Requisitos de formação e treino

Conforme secção 5.3.3 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.4 Frequência e requisitos para ações de reciclagem

Conforme secção 5.3.4 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.5 Frequência e sequência da rotação de funções

Conforme secção 5.3.5 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.6 Sanções para ações não autorizadas

Conforme secção 5.3.7 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.7 Requisitos para prestadores de serviços

Conforme secção 5.3.7 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.3.8 Documentação fornecida ao pessoal

Conforme secção 5.3.8 da Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

5.4 Procedimentos de auditoria de segurança

5.4.1 Tipo de eventos registados

Eventos significativos geram registos auditáveis. Estes incluem, pelo menos os seguintes:

- Geração de par de chaves de assinatura para as TSU;
- Pedido de emissão, suspensão e revogação de certificados para as TSU;
- Sincronização UTC do(s) relógio(s);
- Eventos relacionados com segurança, incluindo:
    - Tentativas de acesso (com e sem sucesso) a recursos sensíveis da EVC;
    - Operações realizadas por membros dos Grupos de Trabalho,
    - Dispositivos físicos de segurança de entrada/saída dos vários níveis de segurança.

As entradas nos registos incluem a informação seguinte:

- Número de série do evento;
- Data e hora do evento;
- Identidade do sujeito que causou o evento;
- Descrição do evento.

5.4.2 Frequência da auditoria interna aos registos

Os registos são auditados pelo menos uma vez por ano e, adicionalmente, sempre que se verifiquem suspeitas ou atividades anormais, ou ameaças de algum tipo, identificadas pelo Grupo de Trabalho de Monitorização e Controlo e os Sistemas de controlo de acessos físicos à sala onde se encontram os sistemas da EVC. Ações tomadas baseadas na informação dos registos são também documentadas.

5.4.3 Período de retenção dos registos de auditoria

Os registos são mantidos disponíveis durante pelo menos 2 (dois) meses após processamento, e depois arquivados nos termos descritos na secção 5.5.

5.4.4 Proteção dos registos de auditoria

Os registos são apenas analisados por membros autorizados dos Grupos de Trabalho e protegidos por mecanismos eletrónicos auditáveis de modo a detetar e impedir a ocorrência de tentativas de modificação, remoção ou outros esquemas de manipulação não autorizada dos dados.

A destruição de um arquivo de auditoria só poderá ser levada a cabo na presença de, no mínimo, dois elementos dos grupos de trabalho, sendo um deles, obrigatoriamente, um elemento do Grupo de Trabalho de Auditoria e sempre com autorização prévia do Grupo de Gestão.

5.4.5 Procedimentos para a cópia de segurança dos registos

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade, nomeadamente em *tape* e *storage.*

5.4.6 Sistema de recolha de registos (Interno / Externo)

O processo de tratamento e recolha de registos de auditoria é constituído por uma combinação de processos automáticos e manuais, executados pelos sistemas operativos, pelas aplicações da EVC e pelo pessoal que as opera. Todos os registos de auditoria são armazenados nos sistemas internos da EVC.

5.4.7 Notificação de agentes causadores de eventos

Eventos auditáveis são registados no sistema de auditoria e guardados de modo seguro, sem haver notificação ao sujeito causador da ocorrência do evento.

5.4.8 Avaliação de vulnerabilidades

Os registos auditáveis são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebrar a segurança do sistema.

São realizados dois testes de intrusão por ano de forma a verificar e avaliar vulnerabilidades.

O resultado da análise é reportado ao Grupo de Gestão da PKI CC para rever e aprovar um plano de implementação e correção das vulnerabilidades detetadas.

5.5 Arquivo de registos

5.5.1 Tipo de dados arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

5.5.2 Período de retenção em arquivo

Os dados sujeitos a arquivo são retidos pelo período de tempo de 7 anos, após a expiração do certificado que assinou o selo temporal.

5.5.3 Proteção dos arquivos

O arquivo é protegido de modo a que:

- Apenas os membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo,
- O arquivo é protegido contra qualquer modificação ou tentativa de o remover,
- O arquivo é protegido contra a deterioração do suporte onde é guardado, através de migração periódica para um suporte novo,
- O arquivo é protegido contra a obsolescência do *hardware*, sistemas operativos e outro *software*, pela conservação do *hardware*, sistemas operativos e outro *software* que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal e
- Os arquivos são guardados de modo seguro em ambientes externos seguros.

5.5.4 Procedimentos para as cópias de segurança do arquivo

As cópias de segurança dos arquivos são efetuadas de modo incremental ou total e guardados em dispositivos de memória terciária.

5.5.5 Requisitos para validação cronológica dos registos

Algumas das entradas dos arquivos contêm informação de data e hora. Tais informações de data e hora têm por base uma fonte de tempo segura.

5.5.6 Sistema de recolha de dados de arquivo (Interno / Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7 Procedimentos de recuperação e verificação de informação arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos para verificação da sua integridade

São realizadas de forma automática verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, em caso de erros ou comportamentos imprevistos, realiza-se novo arquivo.

5.6 Recuperação em caso de desastre ou comprometimento

Esta secção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

5.6.1 Procedimentos em caso de incidente ou comprometimento

Em caso de comprometimento ou suspeita de comprometimento de uma chave de assinatura da TSU, são efetuados os seguintes passos:

- A TSU afetada é desligada;
- O certificado associado é imediatamente revogado e disponibilizado na CRL;
- A chave privada é destruída;
- É gerado um novo par de chaves;
- É pedida a emissão de um novo certificado à EC do Cartão de Cidadão;
- A TSU é inicializada com a utilização do novo par de chaves.

Em caso de perda de sincronismo UTC do relógio da TSU, a TSU será desativada, sendo reativada a partir do momento em que a situação normal seja reposta.

Em caso de outro incidente, o mesmo será analisado pelo Grupo de Trabalho de Monitorização e Controlo, numa primeira fase, sendo implementadas as medidas que garantam a segurança do serviço de Validação Cronológica, a continuidade do serviço e a integridade dos selos temporais.

5.6.2 Corrupção dos recursos informáticos, do *software* e/ou dos dados

No caso dos recursos informáticos, *software* e/ou dados estarem corrompidos ou existir suspeita de corrupção, os registos arquivados podem ser obtidos para verificação da integridade dos dados originais.

Se for confirmado que os recursos informáticos, o *software* e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o

restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a EVC do Cartão de Cidadão suspenderá os seus serviços e notificará a Entidade Supervisora.

5.6.3 Capacidade de continuidade da atividade em caso de desastre

A EVC do Cartão de Cidadão dispõe dos recursos de computação, *software*, cópias de segurança e registos arquivados em locais seguros, necessários para restabelecer ou recuperar operações essenciais (emissão de selo temporal e disponibilização da informação necessária à sua validação).

5.7 Procedimentos em caso de extinção da EVC

A EVC do Cartão de Cidadão garante que potenciais disrupções do serviço de validação cronológica serão minimizadas, como resultado da cessação da sua atividade e, em particular, tomará todas as medidas necessárias para continuar a disponibilizar a informação necessária à verificação da validade dos selos temporais emitidas.

Em caso de cessação de atividade como prestador de serviços de Validação Cronológica, a EVC do Cartão de Cidadão deve, atempadamente, com uma antecedência mínima de três meses, proceder ações descritas na secção 9.10 e garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EVC, nomeadamente, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

6 MEDIDAS DE SEGURANÇA TÉCNICAS

Esta secção define as medidas de segurança implementadas para a EVC do Cartão de Cidadão de forma a proteger chaves criptográficas geradas por esta (chaves de assinatura de selo temporal), e respetivos dados de ativação. O nível de segurança atribuído à manutenção das chaves deve ser máximo, para que componentes criptográficos assim como dados de ativação estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

6.1 Gestão do ciclo de vida do par de chaves

A geração do par de chaves da EVC do Cartão de Cidadão para assinatura de selo temporal é processada de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1 Geração do par de chaves

A geração de chaves criptográficas da EVC do Cartão de Cidadão é efetuada nas instalações seguras do Cartão de Cidadão (conforme secção 5.1) por um Grupo de Trabalho, composto por elementos autorizados para tal.

O *hardware* criptográfico, usado para a geração de chaves da EVC do Cartão de Cidadão, cumpre os requisitos *Common Criteria EAL* 4+ e, efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o *hardware*. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores.

6.1.2 Dimensão das chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptoanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização. A dimensão das chaves é a seguinte:

- 3072 bits RSA para a chave associada ao certificado de assinatura de selo temporal.

6.1.3 Geração dos parâmetros da chave pública e verificação da qualidade

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo.

As chaves são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#1.

6.1.4 Algoritmos de assinatura do selo temporal

A assinatura do selo temporal utiliza a função de *hash* SHA-256 e o algoritmo de assinatura RSA (denominado por *sha256-with-rsa*).

6.2 Proteção da chave privada e características do módulo criptográfico

Nesta secção são considerados os requisitos para proteção da chave privada e para os módulos criptográficos da EVC do Cartão de Cidadão. O Cartão de Cidadão implementou uma combinação de controlos físicos, lógicos e procedimentos, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas de assinatura de selos temporais da EVC do Cartão de Cidadão.

6.2.1 Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da EVC do Cartão de Cidadão assim como para o armazenamento das chaves privadas e assinatura dos selos temporais, o Cartão de Cidadão utiliza módulo criptográfico em *hardware* que cumpre a norma *Common Criteria EAL* 4+.

6.2.2 Gestão do ciclo de vida do módulo criptográfico

A segurança do módulo criptográfico de assinatura de selos temporais é garantida durante o seu ciclo de vida.

Em particular, a EVC do Cartão de Cidadão garante que:

a) O módulo criptográfico não foi adulterado durante o seu transporte;

b) O módulo criptográfico não é adulterado enquanto permanece nas instalações seguras da PKI do Cartão de Cidadão;

c) A instalação e ativação das chaves privadas de assinatura no módulo criptográfico é efetuada por elementos de Grupos de Trabalho bem identificados;

d) O módulo criptográfico tem um funcionamento correto;

e) As chaves privadas de assinatura guardadas no módulo criptográfico são apagadas no final do seu ciclo de vida.

6.2.3 Cópia de segurança da chave privada

Não existe cópia de segurança das chaves privadas da EVC do Cartão de Cidadão para assinatura de selos temporais.

6.2.4 Processo para ativação da chave privada

A EVC do Cartão de Cidadão encontra-se *on-line*, sendo que a chave privada de assinatura da TSU é ativada quando o sistema da TSU é ligado. Esta ativação é efetivada através da autenticação no módulo

criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação de dois fatores.

Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.5 Processo para desativação da chave privada

A chave privada de assinatura da TSU é desativada quando o sistema da TSU é desligado. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

6.2.6 Fim de período de vida da chave privada

As chaves privadas da EVC do Cartão de Cidadão são apagadas/destruídas seguindo indicações precisas do fabricante do equipamento onde se encontram armazenadas. Esta operação é efetuada assim que que expirado o período de validade do certificado utilizado para assinar os selos temporais (ou se revogado antes deste período), estabelecido num máximo definido na secção 6.3.3.

Elementos do Grupo de Trabalho de Autenticação, Operação e acompanhados de elemento do Grupo de Trabalho de Auditoria da EVC do Cartão de Cidadão, procedem à destruição das chaves privadas garantindo que não restarão resíduos destas que possam permitir a sua reconstrução. Para tal, utiliza meios apropriados, que garantem a total destruição das chaves privadas da EVC, após terminado o seu período de validade.

6.3 Outros aspetos da gestão do par de chaves

6.3.1 Emissão do certificado digital

O certificado digital que contém a chave pública de validação cronológica – validação do selo temporal - é emitido pela EC de Assinatura Digital Qualificada do Cartão de Cidadão, de acordo com as seguintes práticas e políticas:

- Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão, disponível em https://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.1.1_0002_pt_AsC.pdf
- Politica de Certificado de Validação Cronológica, disponível em https://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.1.2_0007_pt_Root.pdf

6.3.2 Arquivo da chave pública

É efetuada uma cópia de segurança de todos os certificados (contendo as chaves públicas) da EVC do Cartão de Cidadão, pelos membros do Grupo de Trabalho permanecendo armazenadas após a expiração dos certificados correspondentes, para verificação de assinaturas dos selos temporais geradas durante seu prazo de validade.

Este arquivo está disponível *on-line*, conforme secção 2.1.

6.3.3 Períodos de validade do certificado e das chaves

O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que após expiração do certificado as chaves deixam de poder ser utilizadas, dando origem à cessação permanente da sua operacionalidade e da utilização que lhes foi destinada.

Neste sentido, a validade dos certificados de validação cronológica e período em que os mesmos devem ser renovados, é o seguinte:

- validade máxima de seis anos e seis meses, sendo emitido novo, após o primeiro ano de validade (máximo um ano e seis meses).

6.3.4 Renovação de certificado com geração de novo par de chaves

A renovação de chaves do certificado (*certificate re-key*) é o processo em que é gerado um novo par de chaves e submetido o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito da EC de Assinatura Digital Qualificada do Cartão de Cidadão, é designado por renovação de certificado com geração de novo par de chaves.

6.4 Medidas de segurança informáticas

6.4.1 Requisitos técnicos específicos

O acesso aos servidores da EVC do Cartão de Cidadão é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. A EVC do Cartão de Cidadão tem um funcionamento *on-line*, sendo o pedido de emissão de selos temporais efetuado pelos subscritores.

A EVC do Cartão de Cidadão dispõe de dispositivos de proteção de fronteira, nomeadamente sistema *firewall*, que cumprem os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.4.2 Avaliação/nível de segurança

Os vários sistemas e produtos, empregues pela EVC do Cartão de Cidadão são fiáveis e protegidos contra modificações.

O módulo criptográfico em *Hardware* da EVC do Cartão de Cidadão satisfaz a norma EAL 4+ *Common Criteria for Information Technology Security Evaluation*.

6.5 Ciclo de vida das medidas técnicas de segurança

6.5.1 Medidas de desenvolvimento do sistema

As aplicações são desenvolvidas e implementadas por terceiros de acordo com as suas regras de desenvolvimento de sistemas e de gestão de mudanças. Estes, fornecem em âmbito de auditoria, uma metodologia que permite verificar que o *software* da EVC do Cartão de Cidadão não foi alterado antes da sua primeira utilização.

Todas as configurações e alterações ao *software* são executadas e auditadas por membros pertencentes aos Grupos de Trabalho da EVC do Cartão de Cidadão.

6.5.2 Medidas para a gestão da segurança

O Cartão de Cidadão tem mecanismos e/ou Grupos de Trabalho para controlar e monitorizar a configuração dos sistemas da EVC. O sistema da EVC do Cartão de Cidadão, quando utilizado pela primeira vez, é verificado para garantir que o *software* utilizado é fidedigno e legal e que não foi alterado depois da sua instalação.

6.5.3 Ciclo de vida das medidas de segurança

As operações de atualização e manutenção dos produtos e sistemas da EVC do Cartão de Cidadão, seguem o mesmo controlo que o equipamento original e é instalado pelos membros do Grupo de Trabalho com adequada formação para o efeito, seguindo os procedimentos definidos para o efeito.

6.6 Medidas de Segurança da rede

Descrito na secção 6.4.1

7 Verificação de selos temporais

7.1 Verificação a curto e médio prazo

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 (i.e., até 6 anos após a emissão do selo temporal), a validade da chave privada de assinatura pode ser verificada através do estado de revogação do certificado da TSU, via CRL e/ou OCSP disponibilizada pela EC de Assinatura Digital Qualificada do Cartão de Cidadão.

7.2 Verificação a longo prazo

Usualmente um selo temporal deixa de ser verificável após o fim do período de validade do certificado da TSU, porque a Entidade de Certificação que emitiu o certificado deixa de garantir a publicação de dados de revogação, incluindo revogações devidas ao compromisso da chave privada correspondente.

Contudo, a verificação do selo temporal pode ser efetuada após o fim do período de validade do certificado da TSU, se aquando da verificação, se possa concluir que:

- A chave privada da TSU não foi comprometida até ao final do seu período de validade (tal verificação pode ser efetuada via CRL e/ou OCSP);
- Os algoritmos de *hash* utilizados no selo temporal não exibem colisões, à data da verificação;
- O algoritmo de assinatura e o tamanho da chave, com a qual o selo temporal foi assinado, não é criptograficamente atacável à data da verificação.

Se estas condições não puderem ser garantidas, e se o selo não estiver comprometido, a validade de um selo temporal poderá ser mantida através da emissão de novo selo temporal para proteger a integridade do selo anterior.

8 AUDITORIA E AVALIAÇÕES DE CONFORMIDADE

Uma inspeção regular de conformidade a esta DPVC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria da EVC do Cartão de Cidadão.

Para além de auditorias de conformidade, a EVC irá efetuar outras fiscalizações e investigações para assegurar a conformidade da EVC do Cartão de Cidadão com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

8.1 Frequência ou motivo da auditoria

As auditorias de conformidade são realizadas regularmente de acordo com as normas aplicáveis. A EVC precisa de provar, com a auditoria e relatório de conformidade (produzidos por um organismo de avaliação de conformidade), que a avaliação dos riscos foi assegurada, tendo sido identificado e implementado todas as medidas necessárias para a segurança de informação.

8.2 Identidade e qualificações do auditor

O auditor é uma figura independente do círculo de influência da Entidade de Certificação, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infraestruturas de chaves públicas, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras.

O Organismo Nacional de Acreditação (IPAC) é responsável pela credenciação dos Organismos de Avaliação da Conformidade estando estes capacitados para efetuar as avaliações de conformidade resultando dessas avaliações um Relatório de Conformidade (CAR) a ser disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança.

8.3 Relação entre o auditor e a Entidade Validação Cronológica

O auditor e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

Na relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual.

O auditor e a parte auditada (Entidade de Validação Cronológica) não devem ter nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses.

O cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que este poderá aceder a dados pessoais dos subscritores.

8.4 Âmbito da auditoria

O âmbito das auditorias e de outras avaliações inclui a conformidade com os *standards*, com esta DPVC e outras regras, procedimentos e processos aplicáveis.

8.5 Procedimentos após uma auditoria com resultado deficiente

Se duma auditoria resultarem irregularidades/não-conformidades, o auditor procede da seguinte forma:

a) Documenta todas as deficiências encontradas durante a auditoria;

b) No final da auditoria, reúne com os responsáveis da entidade submetida a auditoria e apresenta de forma resumida um relatório de primeiras impressões;

c) Elabora o relatório de auditoria. Este relatório deverá estar organizado de modo a que todas as deficiências sejam escalonadas por ordem decrescente de gravidade/severidade, identificando o requisito normativo que não é cumprido;

d) Depois de apreciado e consolidado, remete uma cópia do relatório de auditoria final, à entidade;

e) Tendo em conta a irregularidades constantes no relatório, a entidade submetida à auditoria envia um plano de ações corretivas de irregularidades, para a Entidade responsável pela Auditoria, no qual devem estar descritas quais as ações, metodologia e tempo necessário para corrigir as irregularidades encontradas;

f) A Entidade Auditora, depois de analisar este relatório, toma uma das seguintes posições, consoante o nível de gravidade/severidade das irregularidades/não-conformidades:

    a. Aceitam os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;

    b. Dá parecer positivo, mas condicionado, permitindo que a entidade continue em atividade por um período máximo de 90 dias, onde após este deve apresentar a evidências de correção das irregularidades;

    c. Dá parecer negativo, revogando de imediato da atividade.

8.6 Comunicação de resultados

A Entidade Auditada deve comunicar os resultados à Entidade Supervisora.

9 OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

Esta secção aborda aspetos de negócio e assuntos legais.

9.1 Taxas

9.1.1 Taxas por emissão de selo temporal

A serem identificadas em proposta formal a efetuar pela EVC do Cartão de Cidadão.

9.1.2 Taxas para outros serviços

A serem identificadas em proposta formal a efetuar pela EVC do Cartão de Cidadão.

9.1.3 Política de reembolso

Nada a assinalar.

9.2 Responsabilidade financeira

9.2.1 Seguro de cobertura

Nada a assinalar.

9.2.2 Outros recursos

Nada a assinalar.

9.2.3 Seguro ou garantia de cobertura para utilizadores

Nada a assinalar.

9.3 Confidencialidade da informação processada

9.3.1 Âmbito da confidencialidade da informação

Declara-se expressamente, como informação confidencial, aquela que não poderá ser divulgada a terceiros:

a) Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;

b) Planos de continuidade de negócio e recuperação;

c) Registos de transações, incluindo os registos completos e os registos de auditoria das transações;

d) Informação de todos os documentos relacionados com a EVC do Cartão de Cidadão (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade do Cartão de Cidadão. Estes documentos são confiados aos recursos humanos dos Grupos de Trabalho da EVC do Cartão de Cidadão com a condição de não serem usados ou divulgados para além do âmbito dos seus deveres nos termos estabelecidos, sem autorização prévia e explícita do Grupo de Gestão do Cartão de Cidadão;

e) Todas as palavras-chave, PINs e outros elementos de segurança relacionados com a EVC do Cartão de Cidadão;

f) A identificação dos membros dos grupos de trabalho da EVC do Cartão de Cidadão;

g) A localização dos ambientes da EVC do Cartão de Cidadão e seus conteúdos.

9.3.2 Informação fora do âmbito da confidencialidade da informação

Considera-se informação de acesso público:

a) Declaração de Práticas de Validação Cronológica,

b) Declaração de Princípios de Validação Cronológica,

c) Toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

A EVC do Cartão de Cidadão permite o acesso a informação não confidencial sem prejuízo de controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

9.3.3 Responsabilidade de proteção da confidencialidade da informação

Os elementos dos Grupos de Trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento escrito do Grupo de Gestão do Cartão de Cidadão.

9.4 Proteção dos dados pessoais

9.4.1 Medidas para garantia da proteção

Os dados pessoais que podem ser utilizados neste serviço, não são alvo de tratamento, apenas são retidos durante o tempo definido por lei e para efeitos de registos de auditoria.

9.4.2 Informação privada

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.

9.4.3 Informação não protegida pela privacidade

É considerada informação não protegida pela proteção de dados, toda a informação fornecida/obtida pelo titular do certificado que seja disponibilizada no selo temporal.

9.4.4 Responsabilidade de proteção da informação privada

O Ministério da Justiça é responsável pela implementação das medidas que garantem a proteção dos dados pessoais, de acordo com o Regulamento Geral de Proteção de Dados.

9.4.5 Notificação e consentimento para utilização de informação privada

Sendo um serviço gratuito, o consentimento do subscritor está implícito ao utilizar o serviço de selo temporal do Cartão de Cidadão.

9.4.6 Divulgação resultante de processo judicial ou administrativo

Nada a assinalar.

9.4.7 Outras circunstâncias para revelação de informação

Nada a assinalar.

9.5 Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem aos selos temporais emitidos, OID, DPVC e PC, bem como qualquer outro documento, propriedade da EVC do Cartão de Cidadão ou da EC de Assinatura Digital Qualificada do Cartão de Cidadão pertencem ao Ministério da Justiça.

9.6 Representações e garantias

9.6.1 Representação e garantias das entidades de validação cronológica

A EVC do Cartão de Cidadão está obrigada a:

a) Realizar as suas operações de acordo com esta Política,

b) Declarar de forma clara todas as suas Práticas de Validação Cronológica no documento apropriado,

c) Proteger as suas chaves privadas de assinatura de selos temporais,

d) Emitir selos temporais de acordo com o RFC 3161,

e) Emitir selos temporais que estejam conformes com os dados de pedido de selo temporal fornecidos pelo subscritor,

f) Garantir a fiabilidade do processo de geração do selo temporal e da sua entrega ao subscritor,

g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de emissão de selos temporais,

h) Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação,

i) Publicar a sua DPVC e as Políticas aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores,

j) Colaborar com as auditorias dirigidas por um Organismos de Avaliação da Conformidade,

k) Operar de acordo com as normas aplicáveis.

9.6.2 Representação e garantias dos subscritores

É obrigação dos subscritores dos selos temporais:

a) Limitar e adequar a utilização dos selos temporais de acordo com a legislação vigente e com o presente documento,

b) Efetuar o pedido de emissão de selos temporais de acordo com o RFC 3161,

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 o assinar 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.

9.6.3 Representação e garantias das partes confiantes

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

a) Limitar a fiabilidade dos selos temporais às utilizações permitidas para as mesmas em conformidade com a legislação vigente 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 comprometida[1],

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 no https://eportugal.gov.pt/.

9.6.4 Representação e garantias das Fontes Legais de Tempo

É obrigação das fontes legais de tempo utilizadas pela EVC do Cartão de Cidadão:

a) Garantir o acesso ininterrupto à hora fornecida,

b) Garantir a disponibilização de mecanismos que possibilitem o sincronismo entre o seu relógio e o relógio utilizado na emissão de selos temporais,

c) Notificar qualquer acontecimento ou situação anómala.

9.7 Renúncia de garantias

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

9.8 Limitações às obrigações

Conforme secção 1.6. da DDPVC - Declaração de Divulgação de Princípios de Validação Cronológica.

9.9 Indemnizações

Nada a assinalar.

9.10 Termo e cessação da atividade

9.10.1 Notificação de cessação de atividade

Deverão ser notificados com um prazo máximo de 3 meses da cessação da atividade:

- Autoridade Nacional de segurança (GNS);
- Utilizadores da EVC;
- Conselho Gestor do SCEE.

A notificação deve incluir a seguinte informação:

- GNS e Conselho Gestor do SCEE.

[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 efectuada após o fim do período de validade do correspondente certificado, consultar secção 7.2 para orientação.

    - Comunicação para efeitos de cancelamento das credenciações de segurança
- Utilizadores de selos temporais:
    - Informar os utilizadores da cessação do serviço.

Será comunicado a todas as partes confiantes, a fim de minimizar quaisquer interrupções causadas pela cessação da atividade.

9.10.2 Cessação de Relações contratuais

Serão cessadas as relações contratuais com todas as entidades terceiras que, de alguma forma, intervenham nas atividades inerentes à EVC do Cartão de Cidadão.

9.10.3 Revogação de Certificados

Serão revogados todos certificados emitidos para a EVC e inutilizadas as suas chaves privadas.

9.10.4 Transferência de obrigações

No caso do termo e cessação do serviço, sem continuidade do serviço por entidade terceira, será transferida a responsabilidade de manter a informação necessária à evidência das operações do prestador de serviços de confiança, garantindo o seu arquivo por 7 anos, para entidade a nomear.

No caso de cessação e termo de atividade pelo atual fornecedor de serviço, mas com continuidade do serviço por outra entidade, será identificada a entidade de prestação de serviços de confiança para a qual podem ser transferidos os utilizadores da EVC e esta dar continuidade ao serviço de confiança.

9.11 Notificação individual e comunicação aos participantes

Todos os participantes devem utilizar métodos razoáveis para comunicar uns com os outros. Esses métodos podem incluir correio eletrónico assinado digitalmente, fax, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação.

No caso de comunicações a transmitir ao cidadão, serão efetuadas através dos *sites* do Instituto dos Registos e Notariado e do https://eportugal.gov.pt/.

9.12 Alterações

Em caso de alterações do organismo/estrutura responsável de gestão da atividade da EVC, esta deve informar tal facto às entidades listadas na secção 9.10.1.

Relativamente aos documentos relacionados com a EVC do Cartão de Cidadão (incluindo esta DPVC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Gestão e apenas são eliminados ou alterados por sua ordem.

Esta DPVC entra em vigor a partir do momento da sua publicação no repositório da PKI do Cartão de Cidadão e será substituída após emissão de uma nova versão.

9.12.1 Procedimento para alterações

No sentido de alterar este documento ou alguma das políticas de certificado, é necessário submeter um pedido formal ao Grupo de Trabalho das Políticas, indicando (pelo menos):

- A identificação da pessoa que submeteu o pedido de alteração,
- A razão do pedido,
- As alterações pedidas.

O Grupo de Trabalho da Política vai rever o pedido feito e, se verificar a sua pertinência, procede às atualizações necessárias ao documento, resultando numa nova versão de rascunho do documento. O novo rascunho do documento é depois disponibilizado a todos os membros do Grupo de Trabalho e às partes afetadas (se alguma) para permitir o seu escrutínio. Contando a partir da data de disponibilização, as várias partes têm 10 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Trabalho da Política tem mais 5 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento, após o que o documento é aprovado e fornecido Grupo de Gestão para validação, aprovação e publicação, tornando-se as alterações finais e efetivas.

9.12.2 Substituição e revogação da DPVC

O Grupo de Gestão pode decidir em favor da eliminação ou emenda de um documento relacionado com a EVC do Cartão de Cidadão (incluindo esta DPVC) quando:

- Os seus conteúdos são considerados incompletos, imprecisos ou erróneos,
- Os seus conteúdos foram comprometidos.

Nesse caso, o documento eliminado será substituído por uma nova versão.

Esta DPVC será substituída por uma nova versão com independência da transcendência das mudanças efetuadas na mesma, de modo que será sempre de aplicação na sua totalidade.

Quando a DPVC ficar revogada será retirada do repositório público, garantindo-se contudo que será conservada durante o período indicado na secção 5.5.2.

9.12.3 Prazo e mecanismo de notificação

No caso que o Grupo de Gestão julgue que as alterações à especificação podem afetar a aceitabilidade dos selos temporais para propósitos específicos, comunicar-se-á aos utilizadores que se efetuou uma mudança e que devem consultar a nova DPVC no repositório estabelecido.

9.12.4 Motivos para mudar de OID

O Grupo de Trabalho da Política deve determinar se as alterações à DPVC obrigam a uma mudança no OID da política ou no URL que aponta para a DPVC.

Nos casos em que, a julgamento do Grupo de Trabalho da Política, as alterações da DPVC não afetem à aceitação dos selos temporais, proceder-se-á ao aumento do número menor de versão do documento e o último número de Identificador de Objeto (OID) que o representa, mantendo o número maior da versão do documento, assim como o resto de seu OID associado. Não se considera necessário comunicar este tipo de modificações aos subscritores.

No caso em que o Grupo de Trabalho da Política julgue que as alterações à especificação podem afetar a aceitabilidade dos selos temporais para propósitos específicos, proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos subscritores segundo o estabelecido no ponto 9.12.3.

9.12.5 Consequências da cessação de atividade

Após o Grupo de Gestão decidir em favor da eliminação de um documento relacionado com a EVC, o Grupo de Trabalho das Políticas tem 30 dias úteis para submeter para aprovação pelo Grupo de Gestão um documento substituto.

As obrigações e restrições que estabelece esta DPVC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da EVC do Cartão de Cidadão, nascidas sob sua vigência, subsistirão após sua substituição ou revogação por uma nova versão em tudo o que não se oponha a esta.

9.13 Disposições para resolução de conflitos

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

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

9.14 Legislação aplicável

Remete para o regulamento (EU) 910/2014 e *standards* aplicáveis, referidos na seção das Referências Bibliográficas deste documento.

9.15 Conformidade com a legislação em vigor

Esta DPVC é objeto de aplicação de leis nacionais e Europeias, regras, regulamentos, ordenações, decretos e ordens incluindo, mas não limitadas a, restrições na exportação ou importação de *software*, *hardware* ou informação técnica.

É responsabilidade da Entidade Supervisora zelar pelo cumprimento da legislação aplicável listada na secção 9.14.

9.16 Providências várias

9.16.1 Acordo completo

Todas as partes confiantes assumem na sua totalidade o conteúdo da última versão desta DPVC.

9.16.2 Independência

No caso que uma ou mais estipulações deste documento sejam ou tendam a ser inválidas, nulas ou irreclamáveis, em termos jurídicos, deverão ser consideradas como não efetivas.

A situação anterior é valida, apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade da Entidade Supervisora a avaliação da essencialidade das mesmas.

9.16.3 Severidade

Nada a assinalar.

9.16.4 Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

9.16.5 Força Maior

Nada a assinalar.

9.17 Outras providências

Nada a assinalar.

Conclusão

Este documento define os procedimentos e práticas utilizadas pela Entidade de Validação Cronológica do Cartão de Cidadão no suporte à sua atividade de emissão de selos temporais.

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 (CAdES)*, 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 – V1.1.1 (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) 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*

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 58/2019Assegura 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