multicert
Engineering for digital security

Declaração de Práticas de Validação Cronológica

Políticas

MULTICERT_PJ.CA3_24.1.1_0002_pt.doc

Identificação do Projeto: TSA

Identificação da CA: PKI MULTICERT

Nível de Acesso: Público

Versão: 4.0

Data: 26/04/2017

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edifício 3, Piso 3 - 2740-266 Porto Salvo – Oeiras
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

Identificador do documento: MULTICERT_PJ.CA3_24.1.1_0002_pt.doc

Palavras-chave: 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: 26/04/2017

Versão atual: 4.0

Identificação do Projeto: TSA

Identificação da CA: PKI MULTICERT

Cliente: -

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	18/02/2009	Versão inicial	MULTICERT S.A.
1.1	04/08/2009	Atualização do documento, de acordo com alterações efetuadas na plataforma técnica da Entidade de Validação Cronológica	MULTICERT S.A.
1.2	06/06/2014	Revisão	MULTICERT S.A.
2.0	01/08/2014	Versão Aprovada	MULTICERT S.A.
2.1	15/07/2015	Revisão	MULTICERT S.A.
3.0	22/03/2016	Versão Aprovada	MULTICERT S.A.
3.1	16/04/2016	Inclusão das Obrigações das Entidades Externas	MULTICERT S.A.
4.0	26/04/2017	Versão Aprovada	MULTICERT S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_ECRAIZ_127	Declaração de Práticas de Certificação MULTICERT *Trust Services Certificate Authority*	MULTICERT S.A.
MULTICERT_PJ.CA3_24.1.2_0004_pt	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 pessoas, empresas, organizações não, governamentais e o Estado, com vista ao fortalecimento da sociedade de informação, do governo eletrónico (*eGovernment*) e do comércio eletrónico, os selos temporais (*time-stamps*) emitidos pela Entidade de Validação Cronológica da MULTICERT, credenciada pela Autoridade Credenciadora (conforme previsto na legislação europeia e nacional), fornecem os mecanismos necessários para comprovar que um *datum* (conjunto de informação em formato eletrónico) existia na data da aposição do selo temporal.

A infraestrutura da Entidade de Validação Cronológica da MULTICERT fornece selos temporais e mecanismos de validação cronológica, de acordo com a legislação nacional e europeia, conforme com o *standard* ETSI TS 102 023 [4], estando devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014), conforme previsto na legislação portuguesa e europeia, e deste modo habilitada legalmente a emitir todo o tipo de selos temporais, incluindo os selos temporais emitidas por Entidades de Certificação que emitem certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação).

Este documento define os procedimentos e práticas utilizadas pela Entidade de Validação Cronológica da MULTICERT 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 MULTICERT.

Sumário

Introdução

Objetivos

O objetivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Validação Cronológica da MULTICERT (, adiante denominada de EVC, 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 PKI da MULTICERT;
- Terceiras partes, encarregues de auditar a EVC da MULTICERT;
- Todo o público, em geral.

Estrutura do Documento

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

Os primeiros sete capítulos são dedicados a descrever os procedimentos e práticas mais importantes no âmbito dos serviços da EVC. O capítulo oito descreve auditorias de conformidade e outras avaliações. O capítulo nove descreve 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 MULTICERT na emissão de selos temporais e fornecimento de mecanismos de validação cronológica e, explica o que um selo temporal fornece e significa, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos selos emitidos pela MULTICERT. Este documento pode sofrer atualizações regulares.

Os selos emitidos pela MULTICERT contêm uma referência ao DPVC de modo a permitir que Partes confiantes e outras pessoas interessadas possam encontrar informação sobre o selo e sobre 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* (conjunto de informação em formato eletrónico), 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, já que as Entidades de Certificação não revogam certificados após o final do período de validade do certificado.

Um modo de resolver este problema passa pela utilização do selo temporal que permite provar que um *datum* existia antes de um determinado 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.

No entanto, convém salientar que estas práticas e políticas permitem a resolução de outras necessidades.

O selo temporal caracterizado também no "*ETSI Electronic Signature Format standard TS 101 733*" [2] criado com base no "*RFC 3161 – Time-Stamp Protocol*" [13]. Estes documentos identificam os requisitos mínimos de segurança e de qualidade necessários para a garantir a validação confiável de assinaturas eletrónicas de longo prazo.

A Diretiva 1999/93/EC do Parlamento Europeu, define prestador de serviços de certificação como "uma entidade ou uma pessoa singular ou coletiva que emite certificados ou presta outros serviços relacionados com assinaturas eletrónicas". 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.

Os selos temporais são emitidos a pedido dos subscritores e de acordo com o RFC 3161 [13] e são também utilizadas pelas Partes Confiantes para validação da associação da data/hora ao *datum*.

1.1.2 Utilização não autorizada

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

Os serviços de certificação oferecidos pela MULTICERT, não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram um atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

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 que respeita e implementa os seguintes *standards*:

- ETSI TS 102 023: *Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*, v1.2.2 [4];
- RFC 3161 – *Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)* [13];

e cumpre com os requisitos definidos nos documentos:

- ETSI TS 101 861: *Time stamping profile*, v1.3.1 [3];
- CWA 14167-1: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements* [1];
- RFC 3161: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* [15].

Este documento especifica as práticas e políticas de operação e gestão da EVC, 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 da MULTICERT, sendo o valor do OID associado a este documento o 1.3.6.1.4.1.25070.1.2.1.0.1

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 4.0
Estado do Documento	Aprovado

OID	1.3.6.1.4.1.25070.1.2.1.0.1
Data de Emissão	26/04/2017
Validade	1 ano
Localização	https://pki.multicert.com/index.html

1.4 Participantes na Validação Cronológica

1.4.1 Entidade de Validação Cronológica

A MULTICERT TS CA é uma entidade certificadora credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014, conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de selos temporais.

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. No caso da EVC da MULTICERT, o relógio utilizado para emitir selos temporais está sincronizado com pelo menos os relógios atómicos do Observatório Astronómico de Lisboa (OAL) – instituição que tem a incumbência legal de manter e distribuir a Hora Legal em Portugal;

A EVC da MULTICERT é um prestador de serviços de certificação, conforme definido no artigo 2(11) da Diretiva 1999/93/EC do Parlamento Europeu, que emite selos temporais.

1.4.2 Subscritor

O subscritor pode ser uma organização (pessoa coletiva) com vários utilizadores finais ou um utilizador final individual (pessoa singular).

Quando o subscritor é uma organização, algumas das obrigações que se aplicam à organização também se aplicarão aos seus utilizadores finais. Em qualquer caso, a organização será tida como responsável se as obrigações dos seus utilizadores finais não forem cumpridas, pelo que é expectável que a organização informe os seus utilizadores finais sobre as suas obrigações.

Quando o subscritor é um utilizador final, é responsável pelo cumprimento das suas obrigações, conforme secção 9.6.2.

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.

1.4.4 Outros participantes

1.4.4.1 Fonte Legal de Tempo

O relógio utilizado para emitir selos temporais está sincronizado com, pelo menos, os relógios atómicos do Observatório Astronómico de Lisboa (OAL) – instituição que tem a incumbência legal de manter e distribuir a Hora Legal em Portugal (http://oal.ul.pt/); Espanha (http://www.hora.es/) e Brasil (http://http://www.nic.br/).

1.4.4.2 Autoridade Credenciadora

A Autoridade Credenciadora é a entidade competente para a credenciação e fiscalização das entidades certificadoras e entidades de validação cronológica.

De uma forma geral o papel da Autoridade Credenciadora, exercida em Portugal pela Autoridade Nacional de Segurança (ANS), está relacionado com a auditoria/inspeção de conformidade, no sentido de aferir se os processos utilizados pelas EC nas suas atividades de prestação de serviços de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos na legislação portuguesa e europeia, assim como com o estabelecido nesta DPVC.

A Autoridade Credenciadora é uma das "peças" que contribui para a confiabilidade dos selos temporais, pelas competências que exerce sobre as EVC que os emitem. No âmbito das suas funções, a Autoridade Credenciadora, exerce os seguintes papéis relativamente às EVC:

a) Credenciação: procedimento de aprovação da EVC para exercer a sua atividade, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, o HW e SW, os procedimentos de acesso e de operação;

b) Registo: procedimento sem o qual a EVC não poderá emitir selos temporais, na qualidade de EC que emite Certificados Qualificados;

c) Fiscalização: procedimento assente em inspeções efetuadas às EVC, com vista a regularmente verificar parâmetros de conformidade;

d) Credenciação do Auditor de Segurança, figura independente do círculo de influência da EVC e que lhe é exigida.

1.4.4.3 Auditor de Segurança

Figura independente do círculo de influência da Entidade de Certificação, exigida pela Autoridade Credenciadora. A sua missão é auditar a infraestrutura da Entidade de Certificação e Entidade de Validação Cronológica, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, em Março, à Autoridade Credenciadora. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Entidade Credenciadora podem ser encontrados em http://www.gns.gov.pt/media/3992/ListagemdeAS.pdf.

1.4.4.4 Entidades externas de prestação de serviços

As Entidades que prestam serviços de suporte à EVC MULTICERT, têm as suas responsabilidades devidamente definidas através de contratos estabelecidos com as mesmas.

1.5 Política de Validação Cronológica

Uma política de validação cronológica é um "conjunto de regras que indica a aplicabilidade de um selo temporal a uma comunidade particular e/ou conjunto de aplicações com os mesmos requisitos comuns de segurança".

O presente documento define a política e práticas de validação cronológica seguidas pela EVC da MULTICERT na emissão de selos temporais, baseada em certificados digitais e com uma precisão de um segundo.

A EVC da MULTICERT emite selos temporais qualificadas de acordo com as regras e requisitos da Diretiva 1999/93/CE [9] para validade de longo prazo (como definido na TS 101 733 [2]).

O selo temporal emitido pela EVC da MULTICERT inclui o OID da política de Validação Cronológica (1.3.6.1.4.1.25070.1.2.1.0.2), 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 é da responsabilidade do Grupo de de Trabalho de Autenticação da PKI da MULTICERT.

1.6.2 Contato

NOME	Grupo de de Trabalho de Autenticação da PKI da MULTICERT
Morada	MULTICERT S.A. Lagoas Park, Edifício 3, Piso 3 2740-266 Porto Salvo – Oeiras
Correio eletrónico	pki.documentacao@multicert.com
Página Internet	www.multicert.com
Telefone	+351 217 123 010

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

O Grupo de Trabalho de Autenticação 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

A validação desta DPVC (e/ou respetivas PCs) e seguintes correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Autenticação. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPVC (e/ou respetivas PCs), substituindo qualquer DPVC (e/ou respetivas PCs) anteriormente definida.

O Grupo de Trabalho de Autenticação 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	
ANSI	*American National Standards Institute*
CA	*Certification Authority* (o mesmo que EC)
CRL	Ver LRC
DL	Decreto Lei
DN	*Distinguished Name*
DPVC	Declaração de Práticas de Validação Cronológica
EAL	*Evaluation Assurance Level*
EC	Entidade de Certificação
EVC	Entidade de Validação Cronológica
GMT	Tempo Médio de Greenwich (*Greenwich Mean Time*)

LRC	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objecto
PC	Política de Validação Cronológica
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infra-estrutura de Chave Pública)
SHA	*Secure Hash Algorithm*
SSCD	*Secure Signature-Creation Device*
TSA	*Time-Stamping Authority* (o mesmo que EVC)

1.7.2 Definições

Definição	
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	Assinatura eletrónica que preenche os seguintes requisitos:

avançada	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.
Autoridade Credenciadora	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 que contém os elementos referidos no artigo 29.º do DL 62/2003 [7] e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24.º do DL 62/2003.
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.
Dados de criação de	Conjunto único de dados, como chaves privadas, utilizado pelo

assinatura	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	Conjunto de informações em formato eletrónico.
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento 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.
Organismo de certificação	Entidade pública ou privada competente para a avaliação e certificação da conformidade dos processos, sistemas e produtos de assinatura eletrónica com os requisitos a que se refere a alínea c) do n.º 1 do artigo 12.º do DL 62/2003.

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* [10].
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1* [11])
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

A MULTICERT é responsável pelas funções de repositório da EVC da MULTICERT, publicando, entre outras, informação relativa às práticas adotadas.

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

- Disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização, garantindo-se durante o tempo da disponibilidade:
  - Mínimo de 99,990% de respostas a pedidos do documento da DPVC;
- Número máximo de pedidos de selos temporais: 40 pedidos/minuto;
- Número médio de pedidos de selos temporais: 10 pedidos/minuto;
- Número máximo de pedidos simultâneos de selos temporais: 20 pedidos;
- Número médio de pedidos simultâneos de selos temporais: 2 pedidos;
- 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 da MULTICERT, disponibiliza sempre a seguinte informação pública *on-line*:

- Cópia eletrónica desta DPVC e Políticas mais atuais da EVC da MULTICERT, assinada eletronicamente, por indivíduo devidamente autorizado:
  - DPVC da MULTICERT disponibilizada no URI: https://pki.multicert.com/index.html
  - DDPVC da MULTICERT disponibilizada no URI: https://pki.multicert.com/index.html.
- Outra informação relevante – URI: https://pki.multicert.com/index.html - que inclui:
- Descrição de compromisso ou suspeita de compromisso da chave privada de assinatura dos selos temporais, assim como perda de calibração UTC do(s) relógio(s) utilizado(s),
- Informação que permita identificar os selos temporais que podem ter sido afetadas, em caso de compromisso das operações da EVC da MULTICERT ou perda de calibração UTC do(s) relógio(s) utilizado(s).

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

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, de acordo com a 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 (acesso somente para leitura). A EVC da MULTICERT 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 no documento Declaração de Divulgação de Princípios de Validação Cronológica, disponível em https://pki.multicert.com/index.html.

Nesta secção, a EVC divulga a todos os seus subscritores e potenciais partes confiantes, os termos e condições da utilização dos serviços de validação cronológica, numa linguagem fácil de entender.

Esta secção resume alguns dos pontos mais importantes, pelo que a leitura desta secção deve ser complementada com a leitura do restante documento.

3.1 Informação de contato

Conforme secção 1.1. da DDVC - Declaração de Divulgação de Princípios de Validação Cronológica (disponível em https://pki.multicert.com/index.html).

3.2 Tipo de Selo Temporal e sua utilização

Conforme secção 1.2. da DDVC - Declaração de Divulgação de Princípios de Validação Cronológica (disponível em https://pki.multicert.com/index.html).

3.3 Limites de confiança

Conforme secção 1.3. da DDVC - Declaração de Divulgação de Princípios de Validação Cronológica (disponível em https://pki.multicert.com/index.html).

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 da MULTICERT 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 1.4.4.1;

d) A hora/data incluída no selo temporal está sincronizada com o tempo UTC, com a precisão definida neste documento;

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 [13];

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:

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

4.2 Sincronização do relógio

A EVC da MULTICERT garante que o(s) relógio(s) que fornece a hora/data a incluir no selo temporal está sincronizada com o tempo UTC, com a precisão indicada. 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;

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;

c) São detetadas as situações em que o tempo indicado n o selo temporal contêm desvios para a precisão definida;

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.

4.3 Processamento do pedido de selo temporal

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

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

5 Medidas de segurança física, de gestão e operacionais

A PKI da MULTICERT implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes nas declarações de Práticas os serviços disponibilizados pela PKI da MULTICERT. 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. Todos estes controlos, não técnicos, de segurança são críticos para garantir a confiança nos selos temporais, pois qualquer falta 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 PKI da MULTICERT 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 o nível (n-1).

As operações na PKI da MULTICERT 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:

e) Paredes em alvenaria, betão ou tijolo;

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

g) Inexistência de janelas;

h) 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 PKI da MULTICERT:

- 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 PKI da MULTICERT 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.

Atividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer atividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita de alta segurança. O acesso a cada nível de segurança requer o uso de um cartão magnético de autenticação (amarelo para o edifício, e vermelho para os outros níveis). Acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias.

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. O *hardware* criptográfico e *tokens* físicos seguros, dispõem de proteção adicional, sendo guardados em cofres e armários seguros cujo acesso é restrito, de acordo com as necessidades de segregação de responsabilidades dos vários Grupos de Trabalho.

5.1.3 Energia e ar condicionado

O ambiente seguro do PKI da MULTICERT possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de,

- Alimentação de energia, garantindo alimentação contínua ininterrupta 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 dentro do 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 PKI da MULTICERT.

5.1.5 Prevenção e proteção contra incêndio

O ambiente seguro da PKI da MULTICERT 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 e alarme de incêndio, estão instalados nos vários níveis físicos de segurança,
- Equipamento fixo e móvel de extinção de incêndios, estão disponíveis e colocados em sítios estratégicos e 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 contendo *software* e dados de produção, informação para auditoria, arquivo ou cópias de segurança 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 implementado mecanismos de proteção contra acidentes (e.g., causados por água ou fogo).

Quando, para efeito de arquivo de cópias de segurança, informação sensível é transportada da zona de alta segurança para o ambiente externo, o processo é executado sob supervisão de pelo 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

Documentos e materiais em papel que contenham informação sensível, cujo seu ciclo de vida tenha terminado, deverão ser eliminados através de 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. Equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Outros equipamentos de armazenamento (discos rígidos, *tapes*, ...) deverão ser devidamente limpos, de modo a não ser possível recuperar nenhuma informação (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 guardados em ambiente seguro em instalações externas, ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir 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 Certificadora e de uma Entidade de Validação Cronológica depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque:

- Dados os requisitos de segurança inerentes ao funcionamento de uma EC/EVC é vital garantir uma adequada segregação de responsabilidades, que minimize a importância individual de cada um dos intervenientes,

- É necessário garantir que a EC/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 MULTICERT TS CA.

5.2.2 Número de pessoas exigidas por tarefa

Conforme secção 5.2.2 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.2.3 Funções que requerem separação de responsabilidades

Conforme secção 5.2.3 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3 Medidas de Segurança de Pessoal

Conforme secção 5.3 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Conforme secção 5.3.1 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.2 Procedimento de verificação de antecedentes

Conforme secção 5.3.2 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.3 Requisitos de formação e treino

Conforme secção 5.3.3 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.4 Frequência e requisitos para ações de reciclagem

Conforme secção 5.3.4 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.5 Frequência e sequência da rotação de funções

Conforme secção 5.3.5 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.6 Sanções para ações não autorizadas

Conforme secção 5.3.7 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.7 Requisitos para prestadores de serviços

Conforme secção 5.3.7 da Declaração de Práticas de Certificação da MULTICERT TS CA.

5.3.8 Documentação fornecida ao pessoal

Conforme secção 5.3.8 da Declaração de Práticas de Certificação da MULTICERT TS CA.

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;
- Categoria do evento;
- Descrição do evento.

5.4.2 Frequência da auditoria de registos

Os registos são analisados e revistos de modo regular, e adicionalmente sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. 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 *tap*e e *storag*e

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 da MULTICERT 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 definido pela legislação nacional.

5.5.3 Proteção dos arquivos

O arquivo é protegido de modo a que:

- Apenas 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 media onde é guardado, através de migração periódica para media novo,

- O arquivo é protegido contra a obsolescência do *hardware*, sistemas operativos e outros *software*, pela conservação do *hardware*, sistemas operativos e outros *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;
- A chave privada é destruída;
- É gerado um novo par de chaves;
- É pedido a emissão de um novo certificado à MULTICERT TS CA;
- 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 ativada, 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 adequado, sendo implementadas as medidas que garantam a segurança do serviço de Validação Cronológica, a continuidade da disponibilidade 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, *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 da MULTICERT suspenderá os seus serviços e notificará a Autoridade Credenciadora.

5.6.3 Capacidade de continuidade da atividade em caso de desastre

A EVC da MULTICERT 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 da MULTICERT 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 da MULTICERT deve, atempadamente, com uma antecedência mínima de três meses, proceder às seguintes ações:

a) Informar a Autoridade Credenciadora;

b) Informar todos os subscritores e partes confiantes, por correio eletrónico e/ou através de informação na sua página Web;

c) Revogar todos os certificados de assinatura em utilização, até dois dias após a cessação do serviço;

d) Destruir todas as chaves privadas em utilização, até dois dias após a cessação do serviço;

e) Efetuar uma notificação final aos subscritores 2 (dois) dias antes da cessação formal da atividade;

f) 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.

Em caso de alterações do organismo/estrutura responsável de gestão da atividade da EVC, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

6 MEDIDAS DE SEGURANÇA TÉCNICAS

Esta secção define as medidas de segurança implementadas para a EVC da MULTICERT 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 chaves privadas e chaves seguras 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 da MULTICERT 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 da MULTICERT é efetuada nas instalações seguras da MULTICERT TS CA (conforme secção 5.1) por um Grupo de Trabalho, composto por elementos autorizados para tal, numa cerimónia planeada e auditada de acordo com procedimentos escritos das operações a realizar. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos envolvidos no Grupo de Trabalho.

O *hardware* criptográfico, usado para a geração de chaves da EVC da MULTICERT, cumpre os requisitos FIPS 140-1 nível 3 e/ou *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:

- 2048 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 da MULTICERT. A MULTICERT 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 da MULTICERT.

6.2.1 Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da EVC da MULTICERT assim como para o armazenamento das chaves privadas e assinatura dos selos temporais, a MULTICERT utiliza módulo criptográfico em *hardware* que cumpre as seguintes normas:

- Segurança Física
    - *Common Criteria EAL* 4+ e/ou
    - FIPS 140-1, nível 3.

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 da MULTICERT 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 MULTICERT;

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 da MULTICERT para assinatura de selos temporais.

6.2.4 Processo para ativação da chave privada

A EVC da MULTICERT 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 da MULTICERT são apagadas/destruídas num procedimento devidamente identificado e auditado assim que terminada o seu período de utilização (ou se revogadas antes deste período), estabelecido num máximo de dois meses (conforme secção 6.3.3).

A EVC da MULTICERT procede à destruição das chaves privadas garantindo que não restarão resíduos destas que possam permitir a sua reconstrução. Para tal, utiliza a função de formatação (inicialização a zeros) disponibilizada pelo *hardware* criptográfico ou outros meios apropriados, de forma a garantir a total destruição das chaves privadas da EVC, após terminado o seu período de utilização.

O processo operacional e técnico estabelecido garante que todos os meses (ou no máximo, todos os dois meses):

- Um novo par de chaves é gerado e passa a ser utilizado pela TSU,
- É destruído o par de chaves anteriormente em uso,
- A aplicação de geração de selos temporais rejeita qualquer tentativa de emissão de selos temporais se a chave privada tiver expirado.

6.3 Outros aspetos da gestão do par de chaves

6.3.1 Emissão do certificado digital

O certificado digital (contém a chave pública de validação cronológica – validação do selo temporal) é emitido pela MULTICERT TS CA, incluído na hierarquia de confiança da PKI da MULTICERT, de acordo com as seguintes práticas e políticas:

- MULTICERT_PJ.ECRAIZ_127, Declaração de Práticas de Certificação da MULTICERT TS CA,
- MULTICERT_PJ.CA3_24.1.2_0004_pt, Politica de Certificado de Validação Cronológica.

A emissão do certificado é efetuada em cerimónia programada, onde estão presentes, pelo menos, 2 elementos do Grupo de trabalho de Autenticação, 1 de Operação e 1 de Auditoria.

Previamente o Grupo de trabalho de Operação gerou o pedido de certificado e entregou este, ao Grupo de Trabalho de Autenticação que o levará como artefacto para a cerimónia onde será emitido o certificado para este pedido.

Após a emissão do certificado, este é entregue ao Grupo de Operação o qual o irá submeter no serviço de validação cronológica.

6.3.2 Arquivo da chave pública

É efetuada uma cópia de segurança de todos os certificados (contendo as chaves públicas) da EVC da MULTICERT, 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.

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 6 anos e 4 meses, sendo utilizados durante os seus 4 primeiros meses de validade e reemitidos a cada 4 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 MULTICERT TS CA, 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 da MULTICERT é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. A EVC da MULTICERT tem um funcionamento *on-line*, sendo o pedido de emissão de selos temporais efetuado pelos subscritores.

A EVC da MULTICERT dispõe de dispositivos de proteção de fronteira, nomeadamente sistema *firewall*, assim como 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 da MULTICERT são fiáveis e protegidos contra modificações.

O módulo criptográfico em *Hardware* da EVC satisfaz a norma EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-1 nível 3.

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.

É fornecido metodologia auditável que permite verificar que o *software* da EVC da MULTICERT não foi alterado antes da sua primeira utilização. Toda a configuração e alterações do *software* são executadas e auditadas por membros do Grupo de Trabalho.

6.5.2 Medidas para a gestão da segurança

A MULTICERT tem mecanismos e/ou Grupos de Trabalho, para controlar e monitorizar a configuração dos sistemas da EVC. O sistema da EVC da MULTICERT, 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 da MULTICERT, 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

A EVC da MULTICERT dispõe de dispositivos de proteção de fronteira, nomeadamente sistema *firewall*, assim como cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

7 Verificação de selos temporais

7.1 Verificação a curto e médio prazo

Qualquer selo temporal é assinado digitalmente pela TSU da EVC da MULTICERT, por um certificado digital com um mínimo de cinco anos de validade. Durante o período de validade do certificado da TSU (i.e., até 5 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 MULTICERT TS CA.

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 efetua 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 assinada não é criptograficamente atacável à data da verificação.

Se estas condições não poderem ser garantidas, 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 PKI da MULTICERT.

Para além de auditorias de conformidade, a MULTICERT irá efetuar outras fiscalizações e investigações para assegurar a conformidade da EVC 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 a legislação[1]. A MULTICERT precisa de provar, com a auditoria e relatório de segurança anuais (produzidos pelo auditor de segurança acreditado), que a avaliação dos riscos foi assegurada, tendo sido identificado e implementado todas as medidas necessárias para a segurança de informação.

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, tendo que submeter um relatório anual, em Março, à Autoridade Credenciadora.

A Autoridade Credenciadora é responsável pela credenciação do Auditor de Segurança, de acordo com os requisitos e qualificações identificados em http://www.gns.gov.pt/assinatura-electronica.aspx/[2]. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Autoridade Credenciadora pode ser encontrada em http://www.gns.gov.pt/media/3992/ListagemdeAS.pdf.

8.3 Relação entre o Auditor e a Entidade Certificadora

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 garantida a inexistência de qualquer vínculo contratual.

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

[1] cf. Decreto Regulamentar n.º 25/2004, de 15 de Julho.

[2] Norma Técnica – D 01, Requisitos para a Credenciação de Auditor de Segurança previstos no Decreto Regulamentar nº 25/2004, de 15 de Julho, Gabinete Nacional de Segurança, 2007

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 o auditor poderá aceder a dados pessoais dos subscritores.

8.4 Âmbito da auditoria

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional e com este DPVC e outras regras, procedimentos e processos.

8.5 Procedimentos após uma auditoria com resultado deficiente

Se duma auditoria resultarem irregularidades, 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 (RPI);

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;

d) Submete o relatório de auditoria à Autoridade Credenciadora para apreciação;

e) Depois de apreciado e consolidado, é remetida uma cópia do relatório de auditoria final (RAF), para a entidade;

f) Tendo em conta a irregularidades constantes no relatório, a entidade submetida à auditoria enviará uma relatório de correção de irregularidades (RCI), para a Autoridade Credenciadora, no qual deve estar descrito quais as ações, metodologia e tempo necessário para corrigir as irregularidades encontradas;

g) A Autoridade Credenciadora depois de analisar este relatório toma uma das três seguintes opções, consoante o nível de gravidade/severidade das irregularidades:

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

    b. Permite que a entidade continue em atividade por um período máximo de 60 dias até à correção das irregularidades antes da revogação;

    c. Revoga imediatamente a atividade.

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 da MULTICERT.

9.1.2 Taxas para outros serviços

A serem identificadas em proposta formal a efetuar pela EVC da MULTICERT.

9.1.3 Política de reembolso

Nada a assinalar.

9.2 Responsabilidade financeira

9.2.1 Seguro de cobertura

A EVC da MULTICERT dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de Abril [7].

9.2.2 Outros recursos

Nada a assinalar.

9.2.3 Seguro ou garantia de cobertura para utilizadores

A EVC da MULTICERT dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de Abril [7].

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) Toda a informação de caráter pessoal proporcionada à EVC durante o processo de registo dos subscritores, salvo se houver autorização explícita para a sua divulgação;

c) Planos de continuidade de negócio e recuperação;

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

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

f) Todas as palavras-chave, PINs e outros elementos de segurança relacionados com a EVC da MULTICERT;

g) A identificação dos membros dos grupos de trabalho da PKI da MULTICERT;

h) A localização dos ambientes da PKI da MULTICERT 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) Toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

A EVC da MULTICERT 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 da MULTICERT.

9.4 Privacidade dos dados pessoais

9.4.1 Medidas para garantia da privacidade

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

9.4.2 Informação privada

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

9.4.3 Informação não protegida pela privacidade

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo titular do certificado que seja disponibilizada no selo temporal.

9.4.4 Responsabilidade de proteção da informação privada

De acordo com a legislação portuguesa.

9.4.5 Notificação e consentimento para utilização de informação privada

De acordo com a legislação portuguesa.

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 da MULTICERT ou da PKI da MULTICERT pertencem à MULTICERT S.A..

9.6 Representações e garantias

9.6.1 Representação e garantias das entidades de validação cronológica

A EVC da MULTICERT está obrigada a:

a) Realizar as suas operações de acordo com esta Declaração de Práticas,

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 [13],

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, conhecimento 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 pela Autoridade Credenciadora,

k) Operar de acordo com a legislação aplicável,

l) Em caso de cessar a sua atividade deverá comunicar esse facto com uma antecedência mínima de três meses à Autoridade Credenciadora,

m) Cumprir com as especificações contidas na legislação sobre Proteção de Dados Pessoais.

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 [13],

c) Aquando da receção do selo temporal pedido, verificar que o selo temporal foi corretamente assinada pela EVC da MULTICERT,

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 MULTICERT S.A..

9.6.3 Representação e garantias das partes confiantes

É obrigação das partes que confiem nos selos temporais emitidas pela EVC da MULTICERT:

a) Limitar a fiabilidade dos selos temporais às utilizações permitidas para os mesmos 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[3],

d) Assumir a responsabilidade na correta verificação dos selos temporais,

e) Notificar qualquer acontecimento ou situação anómala relativa ao selo temporal, utilizando os meios que a MULTICERT TS CA publique no seu sítio Web.

9.6.4 Representação e garantias das Fontes Legais de Tempo

É obrigação das fontes legais de tempo utilizadas pela EVC da MULTICERT:

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.

[3] 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.

9.7 Renúncia de garantias

A EVC da MULTICERT recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas neste DPVC.

9.8 Limitações às obrigações

a) A EVC da MULTICERT responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Artº 26 do DL 62/2003 [7].

b) A EVC da MULTICERT assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação.

c) A responsabilidade da administração / gestão da EVC da MULTICERT assenta sobre base objetivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços

d) A EVC da MULTICERT só responde pelos danos e prejuízos causados pelo uso indevido do selo temporal, quando não tenha consignado no selo temporal, de forma clara reconhecida por terceiros o limite quanto ao possível uso.

e) A EVC da MULTICERT não responde quando o subscritor superar os limites que figuram neste documento quanto às possíveis utilizações do selo temporal.

f) A EVC da MULTICERT não responde se a parte confiante dos selos temporais não cumprir com as suas obrigações,

g) A EVC da MULTICERT não assume qualquer responsabilidade no caso de perca ou prejuízo:

   ii) Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior,

   iii) Ocasionado pela utilização dos selos temporais quando excedam os limites de utilização estabelecidos neste documento,

   iv) Ocasionado pelo uso indevido ou fraudulento dos selos temporais emitidos pela EVC da MULTICERT.

9.9 Indemnizações

De acordo com a legislação em vigor.

9.10 Termo e cessação da atividade

9.10.1 Termo

Os documentos relacionados com a EVC da MULTICERT (incluindo esta DPVC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Trabalho de Gestão e apenas são eliminados ou alterados por sua ordem.

Esta DPVC entra em vigor desde o momento da sua publicação no repositório da MULTICERT TS CA.

Esta DPVC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão.

9.10.2 Substituição e revogação da DPVC

O Grupo de Trabalho de Gestão pode decidir em favor da eliminação ou emenda de um documento relacionado com a EVC da MULTICERT (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 20 anos.

9.10.3 Consequências da cessação de atividade

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

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

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.

9.12 Alterações

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 de Autenticação, indicando (pelo menos):

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

O Grupo de Trabalho de Autenticação 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 15 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Trabalho de Autenticação tem mais 15 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento, após o que o documento é aprovado e fornecido ao Grupo de Trabalho de Gestão para validação, aprovação e publicação, tornando-se as alterações finais e efetivas.

9.12.2 Prazo e mecanismo de notificação

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

9.12.3 Motivos para mudar de OID

O Grupo de Trabalho de Autenticação 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 de Autenticação, as alterações da DPVC não afetem a 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 de Autenticação 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 9.12.2.

9.13 Disposições para resolução de conflitos

Todas as reclamações entre utilizadores e EVC da MULTICERT deverão ser comunicadas pela parte em disputa à Autoridade Credenciadora, com o fim de tentar resolvê-la 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

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

a) Despacho nº 27008/2004, de 14 de Dezembro, publicado no D.R II, nº 302, de 28 de Dezembro;

b) Portaria nº 1350/2004, de 23 de Outubro;

c) Despacho nº 16445/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;

d) Aviso nº 8134/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;

e) Decreto Regulamentar nº. 25/2004, de 15 de Julho [8];

f) Decreto-Lei nº 290-D/99, de 2 de Agosto [6] com as alterações introduzidas pelo Decreto-Lei nº 62/2003, de 3 de Abril [7] e Decreto-lei nº 165/2004, de 6 de Julho;

g) Portaria nº 1370/2000, publicada no D.R . nº 211, II série de 12 de Setembro.

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 Autoridade Credenciadora 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 em 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 Autoridade Credenciadora 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 da MULTICERT no suporte à sua atividade de emissão de selos temporais.

Referências Bibliográficas

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

[2] ETSI TS 101 733. 2008-07, *Electronic Signatures and Infrastructures (ESI);CMS Advanced Electronic Signatures (CAdES)*, v1.7.4.

[3] ETSI TS 101 861. 2006-01, *Time stamping profile*, v1.3.1.

[4] ETSI TS 102 023. 2008-10, *Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*, v1.2.2.

[5] ETSI TS 102 176-1. 2007-11, *Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms*, v2.0.0

[6] *Decreto-Lei n.º 290-D/99*, de 2 de Agosto.

[7] *Decreto-Lei n.º 62/2003*, de 3 de Abril.

[8] *Decreto Regulamentar n.º 25/2004*, de 15 de Julho.

[9] *Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas electrónicas*, Jornal Oficial nº L 013 de 19/01/2000 p. 0012 – 0020.

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

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

[12] *Portaria n.º 701-G/2008, de 29 de Julho*, I Série.

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

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

[15] RFC 3161: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).*

Aprovação

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.

Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.05.31 15:23:50 +01'00'