Declaração de Divulgação de Princípios de Validação Cronológica

Políticas

MULTICERT_PJ.CA3_24.1.13_0001_pt

Identificação do Projeto: TSA

Identificação da CA: PKI da MULTICERT

Nível de Acesso: Público

Versão: 2.0

Data: 01/08/2014

Identificador do documento: MULTICERT_PJ.CA3_24.1.13_0001_pt

Palavras-chave: SVC, Time-Stamping, Declaração de Divulgação de Princípios de Validação Cronológica

Tipologia documental: Políticas

Título: Declaração de Divulgação de Princípios de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 01/08/2014

Versão atual: 2.0

Identificação do Projeto: TSA

Identificação da CA: PKI da MULTICERT

Cliente: --

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	04/08/2009	Versão inicial	MULTICERT S.A.
1.1	07/08/2009	Atualização de Conteúdos	MULTICERT S.A.
1.2	24/08/2009	Correções gerais	MULTICERT S.A.
1.3	06/06/2014	Atualização de Conteúdos	MULTICERT S.A.
2.0	01/08/2014	Versão Aprovada	MULTICERT S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_ECRAIZ_127	Declaração de Práticas de Certificação MULTICERT *Trust Services Certtificate Authority*	MULTICERT S.A.
MULTICERT_PJ.CA3_24.1.2_0004_pt	Política de Certificado de Validação Cronológica	MULTICERT S.A.
MULTICERT_PJ.CA3_24.1.1_0002_pt	Declaração de Práticas de Validação Cronológica	MULTICERT S.A.

Resumo Executivo

Decorrente da implementação de vários programas públicos e privados para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não governamentais e o Estado, com vista ao fortalecimento da sociedade de informação, do governo eletrónico (*eGovernment*) e do comércio eletrónico, os selos temporais (*time-stamps*) emitidos pelo serviço de Validação Cronológica da MULTICERT *Trust Services Certificate Authority* (MULTICERT TS CA), 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 MULTICERT TS CA fornece selos temporais e mecanismos de validação cronológica, de acordo com a legislação nacional e europeia, conforme com o *standard* ETSI TS 102 023 [4].

A MULTICERT TS CA está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/assinatura-electronica.aspx), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de selos temporais, incluindo os selos temporais emitidas por Entidades de Certificação que emitem certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação).

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

A Declaração de Divulgação de Princípios de Validação Cronológica não constitui a totalidade da Declaração de Práticas sob a qual se rege a emissão de selos temporais (*time-stamps*) pela MULTICERT TS CA. Para este efeito deve ser consultada a Declaração de Práticas de Validação Cronológica da MULTICERT *Trust Services Certificate Authority*, disponível em http://ts4pki.multicert.com/index.html.

Sumário

Introdução

Objetivos

Este documento pretende resumir, de forma simples e acessível, as características descritas na Declaração de Práticas de Validação Cronológica da MULTICERT *Trust Services Certificate Authority* (MULTICERT TS CA), no suporte à sua atividade de emissão de selos temporais e fornecimento de mecanismos de validação cronológica.

A MULTICERT TS CA está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/assinatura-electronica.aspx), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de selos temporais, incluindo os selos temporais emitidas por Entidades de Certificação que emitem certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação).

Público-Alvo

Este documento deve ser lido por:

- Clientes do serviço de Validação Cronológica da MULTICERT TS CA,
- 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.

1 Declaração de Divulgação de Princípios

Nesta secção, a Entidade de Validação Cronológica da MULTICERT (EVC) divulga a todos os seus subscritores e potenciais partes confiantes, os termos e condições da utilização dos serviços de validação cronológica, numa linguagem acessível e fácil compreensão.

Esta secção não deverá ser vista como um resumo de todas as práticas e políticas seguidas pela EVC, mas como um resumo de alguns dos pontos mais importantes, pelo que a leitura desta secção deve ser complementada com a leitura da Declaração de Práticas de Validação Cronológica – DPVC – (disponível em http://ts4pki.multicert.com/index.html).

1.1 Informação de contato

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

1.2 Tipo de Selo Temporal e sua utilização

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

Na EVC da MULTICERT as representações, garantias, limitações e obrigações dos vários participantes na Validação Cronológica estão descritas nas secções 9.6, 9.7 e 9.8 da DPVC - Declaração de Práticas de Validação Cronológica (disponível em http://ts4pki.multicert.com/index.html)

A EVC da MULTICERT aceita pedidos de selo temporal dos seus subscritores, de acordo com o RFC 3161 [13]. O algoritmo de *hash* utilizado para representar o *datum* ao qual se vai apor o selo temporal é o SHA-256.

Qualquer selo temporal é assinado digitalmente pela TSU da EVC da MULTICERT, por um certificado digital com um mínimo de cinco anos de validade. Durante o período de validade do certificado da TSU, a validade da chave privada de assinatura pode ser verificada através do estado de revogação do certificado. Se a verificação é efetuada após o período de validade do correspondente certificado, consultar secção 7.2, da DPVC (disponível em http://ts4pki.multicert.com/index.html), para orientação.

1.3 Limites de confiança

A hora indicada no selo temporal emitido pela EVC da MULTICERT tem uma precisão (em relação ao UTC) máxima de 10ms, sendo garantido no mínimo uma precisão de 100ms. Os registos (*logs*) da EVC da MULTICERT são guardados durante 20 anos, estando durante esse tempo disponíveis como evidência de suporte à precisão da hora indicada nos selos temporais.

A plataforma tecnológica dos serviços de validação cronológica está configurada de acordo com os seguintes indicadores e métricas:

- Disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização.

1.4 Obrigação dos subscritores

É obrigação dos subscritores dos selos temporais:

a) Limitar e adequar a utilização dos selos temporais de acordo com a legislação vigente 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 assinar o selo temporal é válida (i.e., não foi comprometida),

e) Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica (*hardware* e *software*) dos serviços de certificação, sem a devida autorização prévia, por escrito, da MULTICERT TS CA.

1.5 Obrigação das partes confiantes

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

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 assinada,

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 meios que a MULTICERT TS CA publique no seu sítio Web.

1.6 Limites de responsabilidade

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

A Limitações às obrigações são as seguintes:

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].

[1] Note-se que durante o período de validade do certificado da TSU, a validade da chave privada de assinatura pode ser verificada através do estado de revogação do certificado da TSU. Se a verificação é efetuada após o fim do período de validade do correspondente certificado, consultar secção 7.2 da DPVC - Declaração de Práticas de Validação Cronológica (disponível em http://ts4pki.multicert.com/index.html) para orientação.

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 eletrónicas 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) Ocasionados pelo uso dos selos temporais quando excedam os limites de utilização estabelecidos neste documento,

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

1.7 Acordos e Declaração de Práticas aplicável

É aplicável o disposta na Declaração de Práticas de Validação Cronológica – DPVC – (disponível em http://ts4pki.multicert.com/index.html).

1.8 Privacidade dos dados pessoais

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

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

1.9 Indemnizações

De acordo com a legislação em vigor.

1.10 Legislação aplicável e Disposições para resolução de conflitos

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

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

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

a) Despacho 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.

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

1.11 Auditoria

As auditorias de conformidade são realizadas regularmente de acordo com a legislação[2]. A EC precisa de provar, com a auditoria e relatório de segurança anuais (produzidos pelo auditor de segurança acreditado), que a avaliação dos riscos foi assegurada, tendo sido identificado e implementado todas as medidas necessárias para a segurança de informação.

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional, com o descrito na secção 8 da DPVC - Declaração de Práticas de Validação Cronológica (disponível em http://ts4pki.multicert.com/index.html), e outras regras, procedimentos e processos.

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

Referências Bibliográficas

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

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

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

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

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

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

[7] Portaria nº 1370/2000, publicada no D.R . nº 211, II série de 12 de Setembro.

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

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

[10] Portaria nº 1350/2004, de 23 de Outubro;

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

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

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

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

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

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

Validação

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

Assinado de forma digital por [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
DN: c=PT, o=MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A., ou=Certificado para pessoa colectiva - Assinatura Qualificada, title=Procurador com poderes indicados na procuração emitida em 16/10/2013 - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, serialNumber=505767457, cn=[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
Dados: 2014.08.21 20:40:01 +01'00'