Declaração de Práticas de Validação Cronológica

Política

MULTICERT_PJ.CA3_24.1.1_0002_pt

Identificação do Projeto: TSA da Multicert

Nível de Acesso: Público

Versão: 6.0

Data: 01/07/2023

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Rua Carlos Pinto Coelho, 13 - 2720-092 Amadora
Telefone: +351 217 123 010

Identificador do documento: MULTICERT_PJ.CA3_24.1.1_0002_pt

Palavras-chave: Declaração de Práticas de Validação Cronológica

Tipologia documental: Política

Título: Declaração de Práticas de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 01/07/2023

Versão atual: 6.0

Identificação do Projeto: TSA da Multicert

Identificação da CA: TSA 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	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.
4.1	23/04/2018	Revisão de conteúdo	MULTICERT S.A.
4.2	21/09/2021	Revisão de conteúdo	Multicert S.A.
5.0	31/03/2022	Versão Aprovada	Multicert S.A.
5.1	30/06/2023	Revisão de contactos, revisão geral	Multicert S.A.
6.0	01/07/2023	Aprovação	Multicert S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_427	Declaração de Práticas de Certificação MULTICERT	MULTICERT S.A.

Sumário

Introdução

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 EN 319 421, estando devidamente credenciada pela Entidade Supervisora (https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5), conforme previsto na legislação portuguesa e europeia, e deste modo habilitada legalmente a emitir selos temporais qualificados.

os selos temporais (time-stamps) emitidos pela Entidade de Validação Cronológica (EVC) da Multicert fornecem os mecanismos necessários para comprovar que um datum (conjunto de informação em formato eletrónico) existia na data da aposição do selo temporal.

1 Âmbito

Este documento define as políticas e práticas utilizadas pela Entidade de Validação Cronológica da Multicert, dora em diante denominada TSA (Time-Stamping Authority), no suporte à sua atividade de emissão de selos temporais e fornecimento de mecanismos de validação cronológica.

Os detalhes técnicos e processuais da TSA estão descritos neste documento, em complemento ao definido na Declaração de Práticas de Certificação geral da Multicert.

Os selos temporais (time-stamps) emitidos pela Multicert estão em conformidade com a norma ETSI EN 319 421 “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps” e ETSI EN 319 422 “Time-stamping protocol and time-stamp token profiles”.

2 Referências

Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de Julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE

ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

ETSI EN 319 421 – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

ETSI EN 319 422 – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

3 Definições e Abreviaturas

3.1 Definições

Item	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, e que permite 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 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.
Certificado Digital	Documento eletrónico que associa os dados de verificação de uma assinatura com o seu titular/subscritor e confirma a identidade de tal titular/subscritor.
Certificado Qualificado	Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I, II III e IV do Regulamento (EU) Nº 910/2014.
Datum	Conjunto de informações em formato eletrónico.
Prestador de Serviços de Confiança	Entidade que fornece um ou mais serviços de confiança. O mesmo que Trust Service Provider.
Relying Party	Qualquer pessoa singular ou entidade legal que confia num selo temporal.

Selo Temporal	Dados num formulário eletrónico que vincula outros dados eletrónicos a uma data/hora em particular estabelecendo a evidência de que esses dados existiam nessa data/hora. O mesmo que timestamp.
Serviço de Confiança	Serviço eletrónico que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços; ou b) Na criação, verificação e validação de certificados para autenticação de sítios web; ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços. O mesmo que Trust Service.
Serviço de Time-stamping	Serviço de confiança para a emissão de timestamps.
Subscritor	Pessoa singular ou entidade legal para a qual o selo temporal é emitido, e a qual se compromete com as obrigações do Subscritor.
Trust Service	Serviço eletrónico que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços; ou b) Na criação, verificação e validação de certificados para autenticação de sítios web; ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços. O mesmo que Serviço de Confiança.
Time-stamp	Dados num formulário eletrónico que vincula outros dados eletrónicos a uma data/hora em particular estabelecendo a evidência de que esses dados existiam nessa data/hora. O mesmo que selo temporal.

TSP (Trust Service Provider)	Entidade que fornece um ou mais serviços de confiança. O mesmo que Prestador de Serviços de Confiança.
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
Validação de Selo Temporal	Declaração da entidade certificadora, que certifica a data e hora de criação, envio, ou receção de um documento eletrónico.

3.2 Abreviaturas

Abreviatura	
BIPM	Bureau International des Poids et Mesures
CA	Certification Authority (o mesmo que EC)
CAB	Conformity Assessment Body
CP	Certificate Policy (o mesmo que PC)
CRL	Certificate Revocation List (o mesmo que LRC)
DN	Distinguished Name
DPVC	Declaração de Práticas de Validação Cronológica
EC	Entidade de Certificação (o mesmo que CA)
EVC	Entidade de Validação Cronológica (o mesmo que TSA)
GMT	Tempo Médio de Greenwich (Greenwich Mean Time)
ICP	Infraestutura de Chave Pública (o mesmo que PKI)
LRC	Lista de Revogação de Certificados (o mesmo que CRL)

NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Identificador de Objeto
PC	Política de Certificados (o mesmo que CP)
PKI	Public Key Infrastructure (o mesmo que ICP)
TSA	Time-Stamping Authority (o mesmo que EVC)
TSP	Trust Service Provider
TSU	Time-stamping unit
UTC	Coordinated Universal Time

4 Conceitos Gerais

4.1 Conceitos Gerais de Requisitos de Política

Este documento considera a norma ETSI EN 319 401 como referência para os requisitos de política genéricos.

Os requisitos desta DPVC (Declaração de Práticas de Validação Cronológica) são baseados na utilização de criptografia de chave pública, certificados digitais e fontes de tempo confiáveis.

Esta DPVC deve ser consultada pelos Subscritores e *Relying Parties*, de forma a obterem detalhes precisos sobre o funcionamento da TSA da Multicert.

4.2 Serviços de Validação Cronológica

A prestação de serviços de selo temporal é dividida nos seguintes componentes de serviços, com a finalidade de classificar os requisitos:

a) Fornecimento de time-stamping – este componente de serviço gera selos temporais.

b) Gestão de time-stamping – este componente de serviço monitoriza e controla a operação dos serviços de time-stamping para assegurar que o serviço é prestado de acordo com o especificado pela TSA. Este componente de serviço é responsável pela instalação e desinstalação do serviço de fornecimento de time-stamping.

4.3 Entidade de Validação Cronológica (TSA)

Um Prestador de Serviços de Confiança que fornece serviços de time-stamping ao público designa-se por TSA.

A TSA é responsável pela prestação dos serviços de time-stamping identificados na secção 4.2, e é responsável pela operação de um ou mais TSU`s (Time-stamping unit) que criam e assinam em nome da TSA.

A TSA é um Prestador de Serviço de Confiança conforme descrito na ETSI EN 319 401, que emite selos temporais.

A Multicert submete a TSA a auditorias anuais, realizadas por um CAB (Conformity Assessment Body) credenciado. O relatório da referida auditoria é enviado à Entidade Supervisora (Gabinete Nacional de Segurança).

4.4 Subscritor

O Subscritor é uma pessoa singular ou coletiva que adquire os selos temporais produzidos pela TSA e que aceita os termos e condições do serviço TSA.

4.5 Política de Selo Temporal e Declaração de Práticas TSA

Esta secção explica os papéis da política e declaração de práticas da TSA, não sendo colocadas restrições quanto à sua forma.

A Política de Selo Temporal é um tipo de Política de Serviço de Confiança conforme especificado na ETSI EN 319 401 aplicável aos Prestadores de Serviço de Confiança que emitem selos temporais.

Este documento especifica a política e declaração de práticas de selo temporal da TSA da Multicert.

5 Políticas de Selo Temporal

5.1 Geral

Esta política define um conjunto de regras seguidas pela Multicert quando emite selos temporais, suportados por certificados digitais, com uma precisão de 1 segundo ou superior em relação ao UTC.

5.2 Identificação

Os identificadores da política de selo temporal especificado neste documento são:

- 1.3.6.1.4.1.25070.1.2.1.0.1 – identificador de Declaração de Práticas de Validação Cronológica
- 1.3.6.1.4.1.25070.1.1.1.0.7 – identificador de Declaração de Práticas de Certificação da Multicert

Ao incluir este identificador, a Multicert indica conformidade com as seguintes políticas de selo temporal adicionais:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023)

policy-identifiers(1) best-practices-ts-policy (1)

Os seguintes identificadores são descontinuados, mas a sua informação passa a estar presente neste documento:

- 1.3.6.1.4.1.25070.1.1.1.2.0.1.1
- 1.3.6.1.4.1.25070.1.1.1.2.0.7

5.3 Comunidade de Utilizadores e Aplicabilidade

Este documento pode ser usado por serviços de time-stamping públicos ou serviços de time-stamping usados numa comunidade fechada.

6 Políticas e Práticas

6.1 Avaliação do Risco

A Multicert realiza avaliações do risco, no mínimo anualmente, onde se inclui entre outros âmbitos, o âmbito da prestação do serviço de confiança de selos temporais. A avaliação do risco inclui:

a) Identificação e análise de ameaças internas e externas que podem resultar em impactos;

b) Avaliação do impacto das ameaças e probabilidade da sua ocorrência;

c) Definição de Plano de Tratamento do Risco, com a identificação das medidas de tratamento do risco selecionadas, de forma a reduzir o risco identificado para um nível aceitável.

6.2 Declaração de Práticas do Serviço de Confiança

A Multicert assegura a qualidade, desempenho, e operação do serviço de time-stamping através da implementação de controlos e políticas de segurança.

Os controlos e políticas de segurança são revistos e auditados regularmente por entidades independentes.

Adicionalmente, para garantia de conformidade com a norma ETSI EN 319 421, estão implementadas as medidas indicadas nas subsecções seguintes.

6.2.1 Formato de Selo Temporal

Os selos temporais emitidos pela Multicert estão em conformidade com o RFC 3161. O serviço emite selos temporais RSA 2048 que utilizam o algoritmo de hash SHA256.

6.2.2 Precisão do Tempo

O serviço de selos temporais utiliza uma appliance UTC, com sincronização por sistema GNSS, com fallback para fontes UTC configuradas, sendo que estas constam sempre na lista do BIPM.

Se a fonte UTC não estiver dentro da precisão indicada, ou seja +/- 1 segundo, o selo temporal não é emitido, sendo que a TSA devolve um erro indicando que a fonte de tempo não está disponível, conforme previsto no RFC 3161.

6.2.3 Limitações do Serviço

Sem estipulação.

6.2.4 Obrigações do Subscritor

É obrigação do Subscritor de selos temporais:

a) Não exceder o número permitido de selos temporais adquiridos;

b) Ser responsável por aplicar os selos temporais nos documentos utilizando o URL fornecido pela Multicert;

c) Não permitir a utilização do serviço por terceiras partes;

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

e) Efetuar o pedido de emissão de selos temporais de acordo com o RFC 3161;

f) Aquando da receção do selo temporal pedido, verificar que o selo temporal foi corretamente assinado pela TSA da Multicert;

g) Aquando da receção do selo temporal pedido, verificar que a chave privada utilizada para assinar é válida (isto é, não foi comprometida);

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

6.2.5 Obrigações das *Relying Parties*

Ver secção 6.6.

6.2.6 Verificação do Selo Temporal

A verificação do selo temporal inclui as verificações descritas nas seguintes subseções.

6.2.6.1 Verificação do Emissor do Selo Temporal

A TSA utiliza certificados digitais apropriados para emissão de selos temporais. Os certificados digitais são emitidos por uma Entidade de Certificação cujo certificado digital se encontra publicado no repositório da Multicert em https://pki.multicert.com.

6.2.6.2 Verificação do Estado de Revogação do Selo Temporal

6.2.6.2.1 Verificação do Estado de Revogação durante a Validade do Certificado TSU

O selo temporal é assinado digitalmente pela TSU da TSA da Multicert, por um certificado digital com validade de 6 anos. Durante o período de validade do certificado TSU, a validade da chave privada de assinatura pode ser verificada através do estado de revogação do certificado da TSU, através dos endereços de acesso ao serviço OCSP e CRL`s que estão identificados no certificado digital que emite os selos temporais.

6.2.6.2.2 Verificação do Estado de Revogação após a Expiração do Certificado TSU

O selo temporal deixa de ser verificável após o fim do período de validade do certificado da TSU, uma vez que a TSA que emitiu o certificado deixa de garantir a publicação de dados de revogação, incluindo revogações devido 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) A chave privada da TSU não foi comprometida até ao final do seu período de validade (tal verificação pode ser efetuada através da CRL e/ou OCSP);

b) Os algoritmos de *hash* utilizados no selo temporal não exibem colisões, à data de verificação;

c) O algoritmo de assinatura e o tamanho da chave com a qual o selo temporal foi assinado não é criptograficamente atacável à data da verificação.

Se estas condições não poderem ser garantidas, a validade de um selo temporal poderá ser mantida através da emissão de um novo selo temporal, para proteger a integridade do selo temporal anterior.

6.2.7 Legislação Aplicável

Esta declaração de práticas é gerida e interpretada de acordo com a legislação Portuguesa e Europeia aplicável.

6.2.8 Disponibilidade de Serviço

Os controlos e medidas de segurança implementados pela Multicert encontra-se descritos na secção 5 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

6.3 Termos e Condições

6.3.1 Política de Serviço de Confiança aplicável

Este documento representa a política de serviço de confiança aplicável. Para mais informação, consultar a secção 5.

6.3.2 Período de Retenção de Registos pelo TSP

A Multicert retém os registos de auditoria (*audit logs*) gerados por um período de 7 anos após a data de expiração do certificado. A Multicert disponibiliza estes registos de auditoria aos Auditores Externos em âmbito de auditoria ou à Entidade Supervisora, quando solicitado.

6.4 Política de Segurança de Informação

A Multicert tem implementada uma Política de Segurança da Informação, que é revista regularmente ou quando ocorram alterações que o justifiquem.

A Política de Segurança da Informação da Multicert está ainda enquadrada num Sistema de Gestão de Segurança da Informação certificado de acordo com a norma ISO/IEC 27001.

6.5 Obrigações da TSA

6.5.1 Geral

A TSA é responsável por:

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

b) Proteger as suas chaves privadas de assinatura de selos temporais;

c) Emitir selos temporais de acordo com o RFC 3161;

d) Emitir selos temporais que estejam conformes com os dados de pedido de selo temporal fornecidos pelo Subscritor;

e) Garantir a fiabilidade do processo de geração do selo temporal e da sua entrega ao Subscritor;

f) 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;

g) Empregar pessoal com qualificações, conhecimento e experiência necessárias para a prestação de serviços de confiança;

h) Publicar esta Declaração de Práticas e Políticas aplicáveis no seu repositório público, garantindo o acesso às versões atuais;

i) Colaborar com as auditorias dirigidas pelo CAB;

j) Operar de acordo com a legislação aplicável;

k) Em caso de cessação de atividade, comunicar esse facto aos intervenientes e dentro da periodicidade indicados na Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com;

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

6.5.2 Obrigações da TSA para com os Subscritores

Este documento não especifica obrigações adicionais para com os Subscritores para além das referidas na secção 6.5.1.

6.6 Informação para as *Relying Parties*

As *Relying Parties* são responsáveis por:

a) Limitar a fiabilidade dos selos temporais às utilizações permitidas para os mesmos, em conformidade com a legislação vigente e aplicável, 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 até ao momento da verificação.

d) Verificar o estado dos selos temporais, de acordo com a secção 6.2.6.

e) Assumir a responsabilidade pela correta verificação dos selos temporais;

f) Notificar qualquer acontecimento ou situação anómala relativa ao selo temporal, utilizando os meios que a Multicert publique na sua Declaração de Práticas de Certificação (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

7 Gestão e Operação da TSA

7.1 Introdução

A Multicert tem implementadas políticas de segurança e procedimentos operacionais para manter a segurança do serviço.

7.2 Organização Interna

Para a operação apropriada do serviço de validação cronológica, a Multicert mantém um conjunto de documentação interna que especifica os controlos operacionais relacionados com a segurança do pessoal, controlo de acessos, avaliação do risco, entre outros. Essa documentação é auditada por auditores independentes confirmando a conformidade do serviço relativamente à norma ETSI EN 319 421.

A entidade legal que fornece o serviço de validação cronológica é a MULTICERT – Serviços de Certificação Electrónica, S.A.

A TSA utiliza sistemas para a qualidade e gestão de segurança da informação apropriados aos serviços de validação cronológica fornecidos.

A TSA é operada por pessoas com o conhecimento e treino necessários ao desempenho do serviço.

7.3 Segurança Pessoal

O pessoal a desempenhar funções na TSA cumpre com os requisitos dispostos na secção 5.3 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

7.4 Gestão de Recursos

A Multicert tem implementadas controlos de segurança para proteção do recursos e recursos de informação utilizados no serviço de validação cronológica.

7.4.1 Gestão de *Media*

O *media* utilizado no serviço de validação cronológica é manuseado de forma segura, de forma a mantê-lo protegido contra dano, roubo, acesso não autorizado ou obsolescência, e em cumprimento das práticas aplicáveis de acordo com a classificação da informação contida no *media*.

A Multicert tem definidos procedimentos para garantir a proteção do *media* contra obsolescência e deterioração. A destruição de *media* segue também procedimentos definidos de forma a garantir a destruição segura do mesmo e a evitar o acesso não autorizado à informação contida.

7.5 Controlo de Acesso

Os acessos aos sistemas da TSA são limitados apenas aos indivíduos autorizados. Em particular:

a) Os privilégios de acesso seguem o princípio de "*least privileges*", tendo os indivíduos apenas acesso ao necessário para o desempenho das suas funções;

b) Os acessos são modificados ou removidos de forma atempada, de acordo com a alocação dos indivíduos nos grupos de trabalho;

c) O acesso a informação e sistemas é restringido de acordo com a Política de Gestão de Controlo de Acessos;

d) Estão implementados controlos de segurança com o objetivo de segregar as funções dos diferentes grupos de trabalho e as permissões que estes têm nos sistemas;

e) Estão implementados mecanismos de autenticação para acesso à informação e sistemas;

f) São retidos registos de auditoria sobre as atividades realizadas nos sistemas, assegurando a identificação da responsabilidade pelas atividades realizadas pelos elementos dos grupos de trabalho;

g) Estão implementados controlos de segurança para proteger os recursos de acessos não autorizado a informação sensível, estando esses controlos de segurança aplicados ao longo do ciclo de vida da informação.

7.6 Controlos Criptográficos

7.6.1 Geral

A Multicert utiliza várias chaves privadas no serviço da TSA. É utilizada uma chave privada para emitir os certificados de selo temporal que são usados pelos TSU`s.

Todas as chaves privadas são armazenadas num *hardware* criptográfico avaliado de acordo com os requisitos FIPS 140-1 nível 3 e/ou Common Criteria EAL 4+.

7.6.2 Geração da Chave TSU

A geração das chaves criptográficas da TSA é efetuada nas instalações seguras da Multicert (conformes com a secção 5.1 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427), pelos elementos dos Grupos de Trabalho, compostos por elementos autorizados para tal, numa cerimónia planeada e auditada de acordo com os procedimentos de operação definidos. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos dos Grupos de Trabalho envolvidos na cerimónia.

O *hardware* criptográfico utilizado para a geração de chaves da TSA cumpre com 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* criptográfico. 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.

O algoritmo de geração da chave TSU, o tamanho da chave de assinatura e o algoritmo de assinatura usado para assinar os selos temporais segue as especificações da norma ETSI TS 119 312.

7.6.3 Proteção da Chave Privada TSU

A chave privada que assina a TSU é gerada e manuseada dentro de um *hardware* criptográfico que cumpre com os requisitos FIPS 140-1 nível 3 e/ou Common Criteria EAL 4+.

É efetuado backup das chaves privadas da TSU, sendo que a realização do backup e armazenamento do mesmo é efetuado apenas por elementos dos Grupos de Trabalho autorizados, sendo necessária a intervenção de diferentes Grupos de Trabalho.

O backup das chaves privadas da TSU é sempre efetuado usando uma conexão direta de *hardware* criptográfico para *hardware* criptográfico.

7.6.4 Certificado de Chave Pública TSU

A Multicert garante a integridade e autenticidade da chave pública da TSU da seguinte forma:

a) A chave pública de verificação da assinatura da TSU está disponível publicamente através de certificado digital. O certificado digital pode ser encontrado no repositório da Multicert em https://pki.multicert.com.

b) O certificado digital que contém a chave pública de verificação da assinatura da TSU é emitido por uma Entidade de Certificação previamente auditada tendo como critério mínimo as normas ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 421 e ETSI EN 319 422, e estando incluída na *trusted list* europeia disponível em https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5.

7.6.5 Renovação de Chave TSU

O período de validade do certificado da TSU não é superior ao período de tempo em que o algoritmo e tamanho de chave escolhido é reconhecido como seguro (ver secção 7.6.2).

7.6.6 Gestão do Ciclo de Vida do Hardware Criptográfico de Assinatura

O *hardware* criptográfico é inspecionado durante o processo de comissionamento para assegurar a sua conformidade e para verificar que não existem evidências do mesmo ter sido adulterado.

A instalação, ativação e duplicação de chaves de assinatura das TSU`s no *hardware* criptográfico é efetuada por elementos de vários Grupos de Trabalho autorizados, sendo estas operações apenas efetuadas nas instalações seguras da Multicert (ver secção 5.1 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com).

A eliminação de *hardware* criptográfico que contém as chaves privadas de assinatura da TSU, é efetuada seguindo os procedimentos definidos com aplicação de técnicas que tornam praticamente impossível a recuperação das chaves.

7.6.7 Fim do Ciclo de Vida da Chave TSU

A validade das chaves privadas usadas nunca excede a validade dos certificados emitidos usando essas mesmas chaves.

7.7 Selo Temporal

A Multicert emite selos temporais qualificados que estão em conformidade com o perfil de selo temporal definido na norma ETSI EN 319 422.

7.7.1 Emissão de Selo Temporal

Os selos temporais são emitidos de forma segura, em particular:

a) A TSU utiliza valores de tempo nos selos temporais que são rastreáveis para o valor real de tempo distribuído por laboratórios UTC constantes no BIPM.

b) O tempo incluído no selo temporal é sincronizado com UTC dentro da precisão de +/- 1 segundo ou superior.

c) Não são emitidos selos temporais caso o relógio da TSA esteja fora da precisão indicada em b), até que o relógio seja novamente sincronizado.

d) Os selos temporais são assinados por uma chave gerada exclusivamente para este propósito.

e) Não são emitidos selos temporais utilizando uma chave privada da TSU cuja validade tenha expirado.

7.7.2 Sincronização de Relógio com UTC

O relógio da TSA é sincronizado com UTC através de NTP. Em particular:

a) É mantida a calibragem do relógio dentro da precisão indicada na secção 7.7.1, ponto b).

b) O relógio da TSU é protegido contra ataques que possam resultar numa alteração não detetada do relógio que o coloquem fora da calibragem.

c) A precisão do relógio da TSU é monitorizada. Caso a precisão do relógio esteja fora dos parâmetros indicados na secção 7.7.1, ponto b), a TSA não emite selos temporais conforme indicado na secção 7.7.1, ponto c).

a) A sincronização do relógio é mantida quando está programado o "*leap second*", conforme notificado pela entidade competente. A mudança para considerar o "*leap second*" é efetuada no último minuto do dia em que o "*leap second*" está programado. É criado um registo do tempo exato em que a mudança ocorreu.

7.8 Segurança Física e Ambiental

A Multicert mantém políticas de segurança física e ambiental para os sistemas utilizados nos serviços da TSA, que abrangem o controlo de acessos físicos, proteção contra desastres naturais, prevenção e proteção contra incêndio, proteção contra falha de energia e comunicações, proteção contra fugas de água, proteção contra roubo ou tentativa não autorizada

de acesso, e *disaster recovery*. Aplica-se o disposto na secção 5.1 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

Estão implementados controlos para proteção do equipamento, informação, media e *software* relacionados com os serviços da TSA.

7.9 Segurança de Operação

A Multicert tem implementados um conjunto controlos de segurança que permitem assegurar a qualidade e disponibilidade do serviço.

Em particular, esses controlos incluem:

a) Análise dos requisitos de segurança no momento de desenho e especificação dos requisitos dos sistemas da TSA.

b) Implementação de procedimentos de controlo de mudança aplicados às *releases*, modificações e *fixes* urgentes do *software* operacional.

c) Proteção da integridade dos sistemas informação da Multicert contra vírus, *software* malicioso ou não autorizado.

d) Definição e implementação de procedimentos para os grupos de trabalho que executam funções no fornecimento do serviço.

e) Especificação de procedimentos para assegurar que os *patches* de segurança são aplicados dentro de um prazo razoável após terem sido disponibilizados. Um *patche* de segurança não necessita ser aplicado caso este introduza vulnerabilidades ou instabilidades que sejam superiores ao benefício da sua aplicação. Neste caso, é documentado o motivo para que o *patche* de segurança não tenha sido aplicado.

f) Monitorização da capacidade de recursos necessária, bem como projeções futuras de necessidades de capacidade, para garantir a disponibilidade necessária de energia e memória.

7.10 Segurança de Rede

A Multicert protege a sua rede e sistema de ataques.

Em particular:

a) A rede é segmentada considerando a relação funcional, lógica e física dos sistemas e serviços de confiança.

b) São aplicados os mesmos controlos de segurança a todos os sistemas existentes na mesma zona segura.

c) É restringido o acesso e comunicações entre zonas apenas ao necessário às operações do TSP. São proibidas ou desativadas as conexões e serviços desnecessários. São revistas regularmente as regras estabelecidas.

d) Os sistemas críticos para a operações enquanto TSP estão localizados em zonas seguras.

e) É separada a rede para administração dos sistemas de IT e a rede operacional do TSP. Os sistemas usados para administração da implementação da política de segurança não são usados para outras finalidades.

f) Os sistemas de produção são separados dos sistemas dos restantes ambientes.

g) A comunicação entre diferentes sistemas de confiança apenas pode ser estabelecida através de canais confiáveis que são logicamente distintos de outros canais de comunicação, e fornecem a identificação segura dos seus *end points* e proteção dos dados do canal contra modificação ou divulgação.

h) A conexão de rede externa à internet é redundante para assegurar a disponibilidade dos serviços em caso de falha.

i) São realizados trimestralmente *scans* de vulnerabilidades a endereços de IP públicos e privados e são registadas evidências de que os *scans* foram realizados por pessoas com conhecimento, ferramentas, código de ética, e a independência necessária para entregar um relatório fidedigno.

j) São realizados testes de penetração anualmente aos sistemas quando é feito o *setup* e após a aplicação de upgrades na infraestrutura ou modificações que a Multicert considere relevantes. São registadas evidências de que os testes de penetração foram realizados por pessoas com conhecimento, ferramentas, código de ética, e a independência necessária para entregar um relatório fidedigno.

k) São implementados controlos (como firewalls) para proteger os domínios internos da Multicert de acessos não autorizados, incluindo acesso por Subscritores ou terceiras partes, e para prevenir todos os protocolos e acessos desnecessários à operação da Multicert enquanto TSP.

l) Os sistemas da TSU são configurados removendo ou desabilitando todas as contas, aplicações, serviços, protocolos e portas que não são usadas nas operações da TSA.

7.11 Gestão de Incidente

As atividades dos sistemas de IT, bem como a sua utilização e pedidos de serviços são monitorizados.

Em particular:

a) A monitorização de atividades tendo em consideração a criticidade da informação existente. É feita monitorização, no mínimo, dos seguintes eventos:

- *Start-up* e *shutdown* de funções de registo (*logs*).
- Disponibilidade e utilização dos serviços necessários na rede do TSP.
- Registos de auditoria (*audit logs*).

b) São detetadas e reportadas por alarmes as atividades anormais que indicam uma potencial violação de segurança, incluindo intrusão na rede dos serviços de confiança.

c) Está definido um processo de gestão de incidentes que é despoletado em caso de ocorrência de incidentes. O processo inclui:

- Identificação e resposta a incidentes detetados.
- Responsáveis pela identificação e resolução de incidentes.
- Notificação de terceiras partes, de acordo com a legislação aplicável.
- Identificação de *root cause* e *lessons learn*.

d) Caso sejam descobertas vulnerabilidades críticas que não tenham ainda sido endereçadas, as mesmas são endereçadas dentro de 48 horas após a sua descoberta.

e) Para cada vulnerabilidade, tendo em consideração o seu impacto potencial:

- É criado e implementado um plano de mitigação; ou
- É documentado com base em factos a razão para a vulnerabilidade não necessitar de mitigação.

7.12 Recolha de Evidência

A Multicert regista e mantém acessíveis os registo de auditoria, de acordo com o disposto na secção 5.4 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

Adicionalmente, são registados todos os eventos relacionados com:

a) O ciclo de vida das chaves TSU.

b) O ciclo de vida dos certificados TSU.

c) A sincronização do relógio da TSU, incluindo informação relacionada com a recalibração normal ou sincronização dos relógios usados nos selos temporais.

d) A deteção da perda de sincronização do relógio.

7.13 Gestão de Continuidade de Negócio

A Multicert tem definido e testado regularmente um Plano de Continuidade de Negócio, que contempla a retoma atempada das atividades enquanto Prestador de Serviços de Confiança.

Este plano contempla a recuperação em caso de comprometimento ou suspeita de comprometimento da chave privada de assinatura da TSU ou perda da calibragem do relógio da TSU, estando incluído entre os procedimentos a desempenhar:

a) A descrição e comunicação do comprometimento que ocorreu aos Subscritores e *Relying Parties*.

b) A paragem da emissão de selos temporais até ter havido uma recuperação do comprometimento.

c) A disponibilização de informação aos Subscritores e *Relying Parties* que lhes permita identificarem os selos temporais que possam ter sido afetados pelo comprometimento, a não ser que esta informação provoque uma quebra da privacidade dos utilizadores da TSA ou da segurança dos serviços da TSA.

7.14 Cessação da TSA e Planos de Cessação

Em caso de cessação de atividade da TSA, a Multicert irá proceder às seguintes ações:

a) Informar a Entidade Supervisora, Subscritores e outras entidades com as quais existem acordos.

b) Publicar a informação sobre a cessação de atividade para as *Relying Parties*.

c) Revogar os certificados TSU.

d) Destruir ou prevenir a utilização, de forma definitiva, das chaves privadas da TSA.

e) Garantir a transferência para retenção de toda a informação relacionada com as atividades da TSA, nomeadamente a chave da TSA, certificados TSU, disponibilidade de CRL`s, documentação armazenada, repositórios e armazenamento de registos de eventos dentro do período definido na secção 5.5.2 da Declaração de Práticas de

Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

7.15 Conformidade

A Multicert assegura o cumprimento das leis e normas aplicáveis, sendo realizadas auditorias anuais por uma entidade independente (CAB) para verificação do seu cumprimento, de acordo com a secção 8 da Declaração de Práticas de Certificação da Multicert (MULTICERT_PJ.ECRAIZ_427) disponível em https://pki.multicert.com.

Em particular, a TSA da Multicert está em conformidade com:

a) Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014;
b) Decreto-Lei nº 12/2021;
c) ETSI EN 319 401;
d) ETSI EN 319 421;
e) ETSI EN 319 422.

8 Requisitos Adicionais para Selos Temporais Qualificados de acordo com o Regulamento (UE) Nº 910/2014

8.1 Certificado de Chave Pública TSU

Os certificados de selo temporal qualificados são emitidos por Entidades de Certificação da Multicert que operam de acordo com a ETSI EN 319 411-2.

8.2 TSA Emissora de Selos Temporais Qualificados e Não Qualificados de acordo com o Regulamento (UE) Nº 910/2014

A Multicert não emite selos temporais não qualificados. Os selos temporais qualificados são emitidos de acordo com o especificado na secção 8.1.

Aprovação

Nuno Ponte (Grupo de Trabalho de Gestão)

[Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte

Digitally signed by [Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte
Date: 2023.07.10 17:37:47 +01'00'