Declaração de Práticas de Certificação da Multicert

Política

MULTICERT_PJ.ECRAIZ_427_pt

Identificação de projeto: MULTICERT PKI

Nível de acesso: Público

Versão: 16.0

Data: 08/09/2023

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

Identificador de documento: MULTICERT_PJ.ECRAIZ_427_pt

Palavras-chave: MULTICERT CA, Declaração de Práticas de Certificação

Tipologia documental: Política

Título: Declaração de Práticas de Certificação

Língua original: Português, English

Língua de publicação: Português, English

Nível de acesso: Público

Data: 08/09/2023

Versão atual: 16.0

Identificação de projeto: MULTICERT PKI

Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	15/06/2018	Revisão de acordo com RFC 3647 e requisitos Baselines CABForum versão 1.5.7	Multicert S.A.
1.1-1.7	25/09/2018	Inclusão de procedimento para prova de controlo de endereço de email. Inclusão de práticas para re-key. Inclusão de declaração sobre CA`s externas	Multicert S.A.
2.0	01/10/2018	Aprovação	Multicert S.A.
2.1	29/01/2019	Proibição de utilização para man-in-middle Revisão de razões de revogação	Multicert S.A.
3.0	29/01/2019	Aprovação	Multicert S.A.
3.1	25/03/2019	Revisão de acordo com Baseline Requirements v1.6.4	Multicert S.A.
4.0	25/03/2019	Aprovação	Multicert S.A.
4.1	25/03/2019	Inclusão informação sobre PSD2	Multicert S.A.
4.2	16/07/2019	Inclusão de informação sobre fatura eletrónica e revisão geral	Multicert S.A.
5.0	16/07/2019	Aprovação	Multicert S.A.
5.1	09/12/2019	Revisão de acordo com Baseline Requirements v1.6.6, inclusão de novas CA`s	Multicert S.A.
6.0	09/12/2019	Aprovação	Multicert S.A.
6.1	06/04/2020	Revisão de acordo com Baseline Requirements v1.6.7,1.6.8,1.6.9	Multicert S.A.
7.0	06/04/2020	Aprovação	Multicert S.A.
7.1	31/08/2020	Revisão de contactos na secção 1.5.2	Multicert S.A.
8.0	31/08/2020	Aprovação	Multicert S.A.
8.1	03/09/2020	Revisão de acordo com BR 1.7.1 e EVBR 1.7.3	Multicert S.A.
9.0	28/09/2020	Aprovação	Multicert S.A.

Versão	Data	Detalhes	Autor(es)
9.1	17/12/2020	Inclusão de informação sobre assinatura digital qualificada e selo eletrónico para fatura eletrónica | Remoção de EC expirada | Revisão de razões de revogação | Revisão de papéis de confiança | Revisão geral de secções 8 e 9	Multicert S.A.
10.0	17/12/2020	Aprovação	Multicert S.A.
10.1	28/04/2021	Clarificação dos métodos que as partes podem usar para demonstrar uma chave privada comprometida, na secção 4.9.12 | Revisão de acordo com BR 1.7.4 e EVBR 1.7.5	Multicert S.A.
11.0	29/04/2021	Aprovação	Multicert S.A.
11.1	29/10/2021	Revisão das práticas TSA | Revisão geral da secção 5 | Atualização de secção 3.2.2.2 métodos de validação de domínio/IP	Multicert S.A.
12.0	31/03/2022	Aprovação	Multicert S.A.
12.1	15/09/2022	Revisão secção 4.8	Multicert S.A.
13.0	02/11/2022	Aprovação	Multicert S.A.
13.1	06/01/2023	Revisão secção 5	Multicert S.A.
14.0	09/01/2023	Aprovação	Multicert S.A.
14.1	13/06/2023	Remoção certificados SSL OV e WC, atualização de contactos	Multicert S.A.
15.0	01/07/2023	Aprovação	Multicert S.A.
15.1	08/09/2023	Revisão secção 3.2. Adicionado método de verificação de identidade Autenticação.gov. Mapeamento entre os métodos de verificação de identidade suportados e as respetivas alíneas do artigo 24º da regulamento eIDAS EU 910/2014.	Multicert S.A.
16.0	08/09/2023	Aprovação	Multicert S.A.

Documentos Relacionados

Identificador de documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_426_pt	Política de Certificado da PKI Multicert	Multicert S.A.
MULTICERT_PJ.CA3_24.1_0001_pt	Declaração de Divulgação de Princípios	Multicert S.A.
MULTICERT_PJ.ECRAIZ_428_pt	Lista de Perfis de Certificado	Multicert S.A.
MULTICERT_PJ.ECRAIZ_405_pt	Política de CA Subordinada	Multicert S.A.
MULTICERT_PJ.ECRAIZ_621_en	Lista de Agências Aprovadas	Multicert S.A.
MULTICERT_PJ.CA3_24.1.1_0002_pt	Declaração de Práticas de Validação Cronológica	Multicert S.A.
MULTICERT:PJ.CA3_24.1.13_0001_pt	Declaração de Divulgação de Princípios de Validação Cronológica	Multicert S.A.

Anexos

Identificador de documento	Detalhes	Autor(es)

Sumário

1 Introdução

1.1 Visão Geral

O presente documento é uma Declaração de Práticas de Certificação, ou DPC, cujo objetivo é a definição de um conjunto de práticas que as Entidades de Certificação (EC`s) da Multicert aplicam para a validação, emissão, gestão e revogação dos certificados por si emitidos. Não sendo objetivo deste documento definir regras legais ou obrigações, mas sim informar, pretende-se que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve as práticas gerais de emissão e gestão de certificados seguida pela Multicert – Serviços de Certificação Eletrónica S.A. e de acordo com a Política de Certificados (PC) definida por esta entidade, explicando o significado e função de um certificado, assim como os procedimentos que deverão ser seguidos pelas *Relying Parties* e por qualquer outra parte interessada em confiar nos certificados emitidos pelas EC`s geridas pela Multicert (PKI Multicert).

Os certificados emitidos na PKI Multicert contêm uma referência à DPC de modo a permitir que as *Relying Parties* e outras partes interessadas possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

Este documento segue a estrutura definida e apresentada pelo grupo de trabalho PKIX (*Public-Key Infrastructure* X.509) do IETF (*Internet Engineering Task Force*) no documento RFC 3647[1].

Os primeiros sete capítulos são dedicados à descrição dos procedimentos e práticas mais importantes no âmbito da certificação digital da PKI Multicert. O capítulo oito descreve as auditorias de conformidade e outras avaliações. O capítulo nove descreve matérias legais.

A PKI da Multicert está em conformidade com a versão atual dos requisitos de *Issuance and Management of Publicly-Trusted Certificates*, publicados pelo CA/Browser Forum no documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", versão identificada na secção 1.6.3, disponibilizado em https://www.cabforum.org. No caso de qualquer inconsistência entre este documento e o descrito no documento de Baselines, o definido no documento emitido pelo CA/Browser Forum sobrepõe-se ao descrito neste documento.

1.2 Designação e Identificação do Documento

Este documento representa a Declaração de Práticas de Certificação (DPC) da PKI Multicert. A DPC é representada num certificado através de um número único designado como "identificador de objecto" (OID). O OID de Política de Certificado é usado conforme explicado na secção 7.1.6.

Este documento é identificado pelos dados constantes na seguinte tabela:

[1] *cf.* RFC 3647. 2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 16.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.0.7
Data de Emissão	08/09/2023
Validade	1 ano
Localização	https://pki.multicert.com/

Para uniformizar a informação correspondente à PKI Multicert, esta DPC, passa a incorporar as DPC`s até agora geridas e disponibilizadas por EC. Neste sentido, os OID`s correspondentes a cada uma dessas DPC`s são descontinuados, mas permanecem válidos durante o ciclo de vida dos certificados já emitidos durante a sua vigência. Os OIDs abaixo indicados são descontinuados, mas a sua informação passa a estar presente neste documento:

- 1.3.6.1.4.1.25070.1.1.1.1.0.7: DPC da Entidade de Certificação Credenciada da Multicert (Multicert Entidade de Certificação 001 e Multicert Certification Authority 002);
- 1.3.6.1.4.1.25070.1.1.1.2.0.7: DPC da Entidade de Certificação de Serviços de Confiança da Multicert (MULTICERT Trust Services Certification Authority 001 e MULTICERT Timestamping Certification Authority 005).

A Multicert emite certificados com os seguintes OID`s:

Tipo de Certificado	OID Multicert
Assinatura Digital Qualificada	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Assinatura Digital Qualificada para Fatura Eletrónica	1.3.6.1.4.1.25070.1.1.1.1.0.1.22
Selo Eletrónico Qualificado	1.3.6.1.4.1.25070.1.1.1.1.0.1.14
Selo Eletrónico Qualificado para Fatura Eletrónica	1.3.6.1.4.1.25070.1.1.1.1.0.1.19
Selo Eletrónico Qualificado PSD2	1.3.6.1.4.1.25070.1.1.1.1.0.1.14 (até 18/10/2019) 1.3.6.1.4.1.25070.1.1.1.1.0.1.18 (após 18/10/2019)
Autenticação	1.3.6.1.4.1.25070.1.1.1.1.0.1.3
Assinatura Digital Avançada	1.3.6.1.4.1.25070.1.1.1.1.0.1.4
Certificado Qualificado de Autenticação de Website	1.3.6.1.4.1.25070.1.1.1.1.0.1.15
Certificado Qualificado de Autenticação de Website PSD2	1.3.6.1.4.1.25070.1.1.1.1.0.1.12

Para além do OID Multicert, os seguintes certificados estão em conformidade com as seguintes Políticas de Certificados normativas:

Tipo de Certificado	Identificador de Objeto (OID)	Descrição
Assinatura Digital Qualificada	0.4.0.194112.1.2	QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD
Selo Eletrónico Qualificado	0.4.0.194112.1.3	QCP-l-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD
Selo Eletrónico Qualificado PSD2	0.4.0.194112.1.1	QCP-l: certificate policy for EU qualified certificates issued to legal persons
Certificado de Autenticação de Website Qualificado e Certificado de Autenticação de Website Qualificado PSD2	0.4.0.194112.1.4	QEVCP-w: certificate policy for EU qualified website authentication certificates based on EVCP
Certificado de Validação Cronológica	0.4.0.2023.1.1	BTSP: a best practices policy for time-stamp

1.3 Participantes PKI

1.3.1 Entidades de Certificação

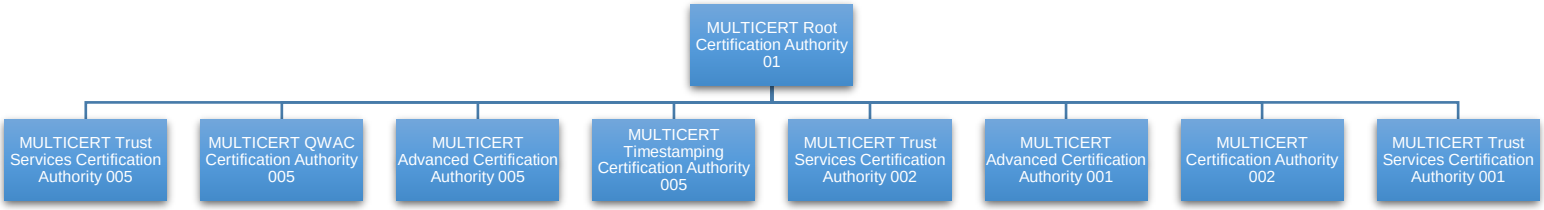
Todas as EC`s públicas geridas pela Multicert estão credenciadas pelo Gabinete Nacional de Segurança (https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitadas legalmente a emitir certificados digitais, incluindo certificados digitais qualificados (certificados digitais com o mais elevado grau de segurança previsto na legislação).

As EC`s geridas pela Multicert são reconhecidas na maioria dos sistemas operativos e navegadores Web, sendo a sua principal função gerir os serviços de certificação: emissão, operação, suspensão, e revogação para os seus Subscritores.

A Multicert gere também uma Entidade de Certificação Timestamping (TSA) que fornece prova de data num determinado momento. As condições específicas da TSA encontram-se descritas no documento Declaração de Práticas de Validação Cronológica (MULTICERT_PJ.CA3_24.1.1_0002_pt) disponível em https://pki.multicert.com.

Esquematicamente, fazem parte da hierarquia da Multicert Root Certification Authority 01 as seguintes EC`s:

EC`s a emitir certificados / com certificados válidos emitidos:



Multicert Root Certification Authority 01

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT
Validade	04/04/2039
Thumbprint	`46 af 7a 31 b5 99 46 0d 46 9d 60 41 14 5b 13 65 1d f9 17 0a`
Emissor	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert Certification Authority 002

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN=MULTICERT Certification Authority 002, OU = Accredited Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT
Validade	19/09/2025
Thumbprint	d5 c7 ec 2e 03 f5 ce a7 b6 3a 3b b4 89 75 92 77 6a 6b f8 d6
Emissor	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert Trust Services Certification Authority 001

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN=MULTICERT Trust Services Certification Authority 001,OU=MULTICERT Trust Services Provider, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validade	01/10/2025
Thumbprint	6d f6 56 30 59 eb 2a 64 3f 74 74 4e 94 56 26 33 92 b8 bf ea
Emissor	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert Advanced Certification Authority 001

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN=MULTICERT Advanced Certification Authority 001,OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validade	12/06/2030
Thumbprint	f8 25 77 a2 a8 c0 fc 1c 57 d2 d8 f3 7e 6c 0f fc 83 b3 3b 09
Emissor	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Multicert Trust Services Certification Authority 002

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN=MULTICERT Trust Services Certification Authority 002,OU=Certification Authority, O=MULTICERT - Serviços de Certificação Electrónica S.A.,C=PT
Validade	12/06/2030
Thumbprint	c8 e5 b7 b4 2d 07 2f 4e 03 fb db 3e 59 8d 51 c1 4c 0a 17 99
Emissor	CN = MULTICERT Root Certification Authority 01,O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

MULTICERT Trust Services Certification Authority 005

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN = MULTICERT Trust Services Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validade	06/08/2032
Thumbprint	75 d1 aa fa d8 82 5c b9 ea ef 92 f7 7f a3 4e 66 e2 ba b6 dc
Emissor	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT QWAC Certification Authority 005

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN = MULTICERT QWAC Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validade	06/08/2032
Thumbprint	14 5d 4b 69 f8 93 99 f0 55 ed 1b b9 c2 62 f2 72 ef b3 d5 9b
Emissor	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT Timestamping Certification Authority 005

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN = MULTICERT Timestamping Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validade	06/08/2032
Thumbprint	50 01 f3 1a 1a b8 b1 56 57 f1 77 7a f8 5b a7 37 b4 dc 93 68
Emissor	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

MULTICERT Advanced Certification Authority 005

INFORMAÇÃO DE CERTIFICADO	
Nome distinto	CN = MULTICERT Advanced Certification Authority 005, OU = Certification Authority, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT
Validade	06/08/2032
Thumbprint	18 8f 27 88 1f ef a7 99 cb f4 9a 1a 79 ad d6 07 f5 56 6e 5d
Emissor	CN = MULTICERT Root Certification Authority 01, O = MULTICERT - Serviços de Certificação Electrónica S.A., C = PT

1.3.1.1 Entidades de Certificação Externas

A definição de políticas e dados para a emissão e gestão de certificados pelas EC`s Subordinadas externas são definidas na Política de EC Subordinada, disponível em https://pki.multicert.com.

1.3.2 Entidades de Registo

A Entidade de Registo (ER) é a entidade que aprova os nomes distintos (DN) dos Subscritores/Titulares dos certificados e mediante avaliação do pedido, aceita ou rejeita a solicitação do certificado. Para além disso, a ER também tem autoridade para aprovar a revogação ou suspensão de certificados.

As Entidades de Registo da PKI Multicert cumprem os requisitos dispostos neste documento e estão sujeitas a Auditorias Externas, efetuadas por auditores CAB, assim como Auditorias Internas, efetuadas pela Multicert.

1.3.2.1 Entidade de Registo Interna

No âmbito da PKI Multicert, a entidade de registo materializa-se pelos serviços internos da mesma que procedem ao registo e validação dos dados necessários, conforme explicitado na secção 3.

1.3.2.2 Entidades de Registo Externas

A PKI Multicert descentraliza esta função através das ER`s externas, que efetuam as seguintes atividades:

- Validação do pedido de certificado;
- A ER é responsável por garantir a entrega das condições gerais de emissão de certificado digital ao Subscritor;
- Após aprovação, a ER é responsável pela submissão do pedido de emissão de certificado à EC Multicert;
- A EC devolve o certificado, customizado usando um dispositivo criptográfico;
- A ER é responsável por garantir a entrega do certificado digital ao Subscritor ou a quem o represente legalmente;
- A ER é responsável por processar pedidos de revogação, e quando aplicável, pedidos de suspensão, e por efetuar o pedido de mudança de estado de certificados digitais imediatamente após o Subscritor cessar funções no âmbito para o qual o certificado foi emitido ou quando se verifica uma das razões de revogação/suspensão constantes na secção 4.9.

1.3.3 Subscritores / Titulares

No contexto deste documento o termo Subscritor / Titular aplica-se a todos os utilizadores finais que tenham adquirido certificados à PKI Multicert.

São considerados Subscritores / Titulares de certificados emitidos pela PKI da Multicert, aqueles cujo nome está inscrito no campo “Assunto” (*Subject*) do certificado e utilizam o certificado e

respetiva chave privada de acordo com o estabelecido neste documento, sendo emitidos certificados para as seguintes categorias de Subscritores / Titulares:

- Pessoa física ou jurídica;
- Pessoa coletiva (Organizações);
- Serviços (como computadores, firewalls, routers, servidores).

Em alguns casos, os certificados são emitidos diretamente a pessoas físicas ou jurídicas para uso pessoal, no entanto, existem situações em que quem solicita o certificado é diferente do Titular do mesmo, por exemplo, uma organização pode solicitar certificados para os seus colaboradores para que estes representem a organização em transações/comércio eletrónico. Nestas situações a entidade/organização que solicita a emissão do certificado é diferente do Titular do mesmo.

1.3.3.1 Patrocinador

A emissão de certificados para equipamentos tecnológicos é efetuada sempre sob responsabilidade humana, sendo esta entidade designada por Patrocinador ou Responsável Técnico do certificado. Neste caso, a ER valida a autoridade do Patrocinador / Responsável Técnico do certificado para representar a entidade/organização.

O Patrocinador tem que aceitar o certificado e é responsável pela sua correta utilização, bem como pela proteção e salvaguarda da sua chave privada.

1.3.4 Relying Parties

As *Relying Parties* ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do Titular com a sua chave pública, ou seja, confiam que o certificado corresponde na realidade a quem diz pertencer.

Neste documento, considera-se uma *Relying Partie*, aquela que confia no conteúdo, validade e aplicabilidade do certificado emitido pela PKI Multicert.

As *Relying Parties* têm que verificar a CRL ou resposta OCSP adequada antes de confiar na informação constante no certificado. A localização do ponto de distribuição da CRL e OCSP está detalhada no certificado.

1.3.5 Outros Participantes

1.3.5.1 Entidade Supervisora

A Entidade Supervisora é a entidade competente para a credenciação e fiscalização das entidades certificadoras.

De uma forma geral o papel da Entidade Supervisora, exercida em Portugal pelo Gabinete Nacional de Segurança (GNS), está relacionado com a supervisão dos prestadores qualificados de serviços de confiança, no sentido de aferir se os serviços de confiança por eles prestados cumprem os requisitos de conformidade.

A Entidade Supervisora é uma das partes que contribui para a confiabilidade dos certificados, pelas competências que exerce sobre as EC`s que os emitem. No âmbito das suas funções, exerce os seguintes papéis relativamente às EC`s:

a) Credenciação: procedimento de aprovação da EC para exercer a sua atividade, com base numa avaliação feita a parâmetros, tais como a segurança física, hardware e software, procedimentos de acesso e de operação;

b) Registo: procedimento sem o qual a EC não pode emitir certificados;

c) Fiscalização: procedimento assente em inspeções/auditorias efetuadas à EC, com vista a verificar parâmetros de conformidade.

1.3.5.2 Entidade de Registo

Detalhado na secção 1.3.2.

1.3.5.3 Entidades Externas de Prestação de Serviços

As Entidades que prestam serviços de suporte à PKI Multicert têm as suas responsabilidades deviamente definidas através de contratos estabelecidos com as mesmas.

1.3.5.4 Entidade de Validação OCSP

A Entidade de Validação OCSP, tem como função comprovar o estado dos certificados emitidos, através da utilização do protocolo *Online Certificate Status Protocol*[2] (OCSP), de forma a determinar o estado atual do certificado, a pedido de uma entidade, sem necessidade de recorrer à verificação do estado através da consulta das Listas de Certificados Revogados (CRL).

O serviço de Entidade de Validação OCSP é disponibilizado pela PKI Multicert.

1.3.5.5 Auditor de um Organismo de Avaliação de Conformidade

Figura independente, externo à Entidade de Certificação, pertencente a um CAB (*Conformity Assessment Body*) acreditado. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras para avaliação de conformidade dos serviços de confiança ao abrigo do Regulamento 910/2014 e critérios aplicáveis.

As Entidades de Certificação geridas pela Multicert são auditadas por um CAB identificado na Lista Europeia de CAB´s (*European Union Listo f Conformity Assessment Bodies*) considerando os requisitos do Regulamento eIDAS[3], que emite um Relatório de Avaliação de Conformidade (*Conformity Assessment Report* – CAR) fornecido à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança.

As auditorias de conformidade ocorrem no mínimo anualmente, para confirmar que a Multicert, como prestador de serviços de confiança está em conformidade com os requisitos definidos no Regulamento 910/2014 e critérios aplicáveis.

1.4 Utilização do Certificado

Os certificados emitidos no âmbito da PKI Multicert são utilizados pelos vários Subscritores/Titulares, sistemas, aplicações, mecanismos e protocolos de forma a garantir os

[2] cf.RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol–OCSP.
[3] Lista disponível em https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/CAB_NAB

seguintes serviços de segurança, dependendo do constante nos campos de utilização da chave e utilização estendida da chave do certificado:

a) Controlo de Acessos/Autenticação;

b) Confidencialidade;

c) Integridade;

d) Autenticidade e;

e) Não-repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através do seu uso na estrutura de confiança que a PKI Multicert fornece. Os serviços de autenticidade, autenticação, integridade e não-repúdio são obtidos através da utilização de assinaturas digitais. A confidencialidade é garantida através do recurso a algoritmos de cifra, juntamente com mecanismos para estabelecer e distribuir chaves.

1.4.1 Utilizações Apropriadas de Certificado

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela PKI Multicert.

Os certificados emitidos de acordo com esta DPC podem ser usados para controlo de acessos/autenticação, confidencialidade, integridade, autenticidade ou não-repúdio, dependendo da utilização de chave e utilização estendida de chave existentes no certificado. A utilização apropriada de cada tipo de certificado encontra-se descrita na seguinte tabela.

Certificado	Utilização Apropriada
Assinatura Digital Qualificada	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Quando o campo Serial Number do Subject Distinguished Name contém o prefixo “TIN”, o certificado deve ser usado para assinatura de faturas eletrónicas e formulários de pedido para a mesma utilização de certificados. Emitido para um indivíduo, com ou sem associação de entidade/organização. Garante o não-repúdio de assinaturas e integridade do conteúdo assinados pelos indivíduos. Esta assinatura tem o mesmo valor legal probatório que uma assinatura manuscrita.
Selo Eletrónico Qualificado	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para entidades legais / organizações. Garante a autenticidade e integridade do conteúdo assinado pelas entidades / organizações.
Selo Eletrónico Qualificado para Fatura Eletrónica	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para entidades legais / organizações. Garante a autenticidade e integridade do conteúdo assinado pelas entidades / organizações.
Autenticação	Utilização específica para autenticação de transações eletrónicas que suportam o acesso a web sites e outro conteúdo online, correio eletrónico, sistemas da organização, etc. Emitido para um indivíduo, com os sem associação de entidade/organização. Garante a autenticidade de indivíduos (com ou sem associação de entidade/organização).

Assinatura Digital Avançada	Utilização para transações que suportam a assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para um indivíduo, com ou sem associação de uma entidade/organização. Garante o não-repúdio de assinaturas e integridade do conteúdo assinado pelos indivíduos. Utilização específica para autenticação de transações eletrónicas que suportam o acesso a web sites e outro conteúdo online, correio eletrónico, sistemas da organização, etc. Emitido para um indivíduo, com os sem associação de entidade/organização. Garante a autenticidade de indivíduos (com ou sem associação de entidade/organização). Utilização para cifrar informação a ser comunicada, tal como documentos eletrónicos ou conteúdo de correio eletrónico. Garante a confidencialidade do conteúdo.
Selo Eletrónico Qualificado PSD2	Utilização para transações que suportam assinatura digital de formulários eletrónicos, documentos eletrónicos, ou correio eletrónico. Emitido para entidades legais / organizações. Garante a autenticidade e integridade do conteúdo assinado pelas entidades / organizações.
Autenticação de Website Qualificado PSD2	Utilização para comunicações *online* seguras em que os riscos e consequências do comprometimento de dados é alto. Associa um nome de domínio a uma organização. Garante a autenticidade e confidencialidade.

Os certificados das EC`s da PKI Multicert são também utilizados pelas *Relying Parties* para verificação da cadeia de confiança de um certificado emitido pelas mesmas, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública incluída num certificado emitido pelas EC`s da PKI Multicert.

1.4.2 Utilizações Proibidas de Certificado

Os certificados podem ser utilizados noutros contextos apenas na extensão do que é permitido pela legislação aplicável.

Os certificados emitidos pela PKI Multicert não podem ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela PKI Multicert não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram uma 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.

Adicionalmente, os certificados emitidos no âmbito desta DPC não podem ser usados para a finalidade de gestão de tráfego ou *man-in-middle*.

Os certificados não garantem que o Sujeito seja confiável, honesto, respeitável nas suas transações comerciais, seguro para fazer negócios, ou em conformidade com quaisquer leis. O certificado apenas estabelece que a informação do certificado foi verificada de acordo com esta DPC quando o certificado foi emitido.

1.5 Gestão da Política

1.5.1 Entidade Responsável pela Gestão do Documento

A gestão desta DPC é da responsabilidade do Grupo de Trabalho de Autenticação da PKI Multicert, que pode ser contactado através dos contactos indicados na secção 1.5.2.

1.5.2 Contacto

NOME	Grupo de Trabalho de Autenticação da PKI Multicert
Morada:	A/C: Grupo de Trabalho de Autenticação Multicert – Serviços de Certificação Electrónica, S.A. Rua Carlos Pinto Coelho, 13 2720-092 Amadora, Portugal
Correio Eletrónico:	ca.forum@multicert.com Para certificados PSD2: psd2@multicert.com
Página Web	https://www.multicert.com
Telefone:	+351 217 123 010

No âmbito dos certificados PSD2, caso a NCA pretenda notificar ou comunicar com o TSP, por exemplo, a respeito da comunicação de alterações às informações regulatórias relevantes para o PSD2, ou caso pretenda ser notificada sempre que um certificado PSD2 é emitido ou revogado, ou caso pretenda solicitar a revogação de certificados PSD2 emitidos para um PSP, a NCA deve usar o correio eletrónico acima referido para comunicações relativamente a certificados PSD2.

Os Subscritores, Relying Parties, Fornecedores de Aplicações de Software, e outras terceiras partes podem reportar a suspeita de comprometimento da chave privada, uso indevido do certificado, ou outros tipos de fraude, comprometimento, uso indevido, conduta inadequada, ou qualquer outro assunto relacionado com os certificados através do envio de email para os contactos acima.

1.5.3 Responsável por Determinar a Conformidade da DPC

O Grupo de Trabalho de Autenticação da PKI Multicert determina a conformidade e aplicabilidade interna desta DPC (e/ou PC) através da sua submissão para aprovação ao Grupo de Trabalho de Gestão.

1.5.4 Procedimentos para Aprovação da DPC

A validação desta DPC (e/ou respetiva PC) e subsequentes correções (ou atualizações) são desempenhadas pelo Grupo de Trabalho de Autenticação. Correções (ou atualizações) são publicadas sob a forma de novas versões desta DPC (e/ou respetiva PC), substituindo qualquer DPC (e/ou respetiva PC) anteriormente definida. O Grupo de Trabalho de Autenticação determina ainda quando é que as alterações na DPC (e/ou respetiva PC) levam a uma alteração nos identificadores dos objetos (OID) da DPC (e/ou respetiva PC).

Após validação, a DPC (e/ou respetiva PC) é submetida ao Grupo de Trabalho de Gestão, que é responsável pela aprovação e autorização de modificações neste documento.

1.6 Definições e Acrónimos

1.6.1 Definições

Item	Definição
Acreditação/Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o cumprimento dos requisitos definidos neste documento para os fins nele previstos.
Autoridade de Acreditação/Entidade de Credenciação	Entidade competente para a credenciação e supervisão de entidades certificadoras.
Entidade de Certificação (EC)	Entidade em que um ou mais usuários confia para criar e atribuir certificados. Uma EC pode ser: i) um provedor de serviços de confiança que cria e atribui certificados de chave pública; ou ii) um serviço de geração de certificado técnico que é usado por um provedor de serviços de certificação que cria e atribui certificados de chave pública.
Política de Certificado (PC)	Conjunto denominado de regras que indica a aplicabilidade de um certificado a uma determinada comunidade e/ou classe de aplicativo com requisitos de segurança comuns.

Declaração de Práticas de Certificação (DPC)	Declaração de práticas que uma Entidade de Certificação aplica para a emissão, gestão, revogação, e renovação ou *re-key* de certificados.
Lista de Revogação de Certificados (CRL)	Lista assinada que indica os certificados que foram revogados por um emissor de certificado.
Conformity Assessment Body (CAB)	Significa uma entidade definida pelo ponto 13 do Artigo 2 do Regulamento nº 765/2008, que é acreditada de acordo com esse Regulamento como sendo competente para realizar avaliações de conformidade de um prestador de serviços de confiança qualificado e os serviços de confiança que o prestador presta.
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.
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.
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Documento Eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Selo Eletrónico	Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos.
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.
Produto de Assinatura Eletrónica	Suporte lógico, dispositivo de equipamento ou seus componentes específicos, destinados a ser utilizados na prestação de serviços de assinatura eletrónica qualificada por uma entidade certificadora ou na criação e verificação de assinatura eletrónica qualificada.
Certificado Avançado	Certificado que oferece a mesma qualidade de um certificado qualificado, no entanto sem os constrangimentos legais implícitos na assinatura qualificada e sem requisito de utilização de um dispositivo seguro para a sua criação. Não confere o valor probatório legal de uma assinatura qualificada.
Selo Eletrónico Avançado	Um selo eletrónico que obedeça aos requisitos estabelecidos no artigo 36.º do Regulamento (EU) nº 910/2014 do Parlamento Europeu e do Conselho.
Assinatura Eletrónica Avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
OCSP *Responder*	Servidor *online* operado sob a autoridade da EC e conectado ao seu repositório para processar pedidos de estado de certificado.
Online Certificate Status Protocol (OCSP)	Um protocolo *online* de verificação de certificado que permite a aplicações de software de *relying parties* determinar o estado de um certificado identificado.
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.
Certificado PSD2	Um certificado qualificado que inclui atributos específicos PSD2.
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.
Infraestrutura de Chaves Públicas (ICP ou PKI)	Conjunto de hardware, software, pessoas, procedimentos, regras, políticas e obrigações utilizadas para facilitar de forma confiável a criação, emissão, gestão, e utilização de certificados e chaves baseadas em criptografia de chave pública.
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.
Selo Eletrónico Qualificado	Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado de selo eletrónico.
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 de Autenticação de Sítio Web Qualificado	Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo IV do Regulamento (EU) Nº 910/2014.
Relying Party	Qualquer pessoa singular ou entidade legal que confia num certificado válido.
Entidade de Registo (ER)	Entidade principalmente responsável pela identificação e autenticação de sujeitos de certificados. A ER pode apoiar no

	processo de solicitação de certificado, processo de revogação, ou em ambos.
EC Raiz	Entidade Certificadora de raiz, cujo certificado de raiz é distribuído por fornecedores de aplicações de software, e que emite certificados de Entidade Certificadora intermédia.
Dados de Criação de Assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
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 geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura 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) iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Assunto	Pessoa singular, dispositivo, sistema, unidade ou entidade legal identificada num certificado como Assunto. O Assunto pode ser o subscritor/titular ou um dispositivo sob o controlo e operação de um subscritor.

EC Intermédia / Subordinada	Entidade Certificadora cujo certificado é assinado pela Entidade Certificadora Raiz, ou outra Entidade Certificadora Subordinada. Uma EC Subordinada normalmente emite certificados para utilizadores ou certificados para outras EC`s Subordinadas.
Subscritor	Pessoa singular ou entidade legal para a qual um certificado é emitido e que está legalmente vinculada por um contrato ou termos e condições.
Entidade Supervisora	Entidade responsável pelas tarefas de supervisão no respetivo Estado Membro, nomeadamente: - Supervisionar os prestadores qualificados de serviços de confiança estabelecidos no território do Estado-Membro que procede à designação por forma a garantir, por meio de atividades de supervisão a priori e a posteriori, que os prestadores e os serviços de confiança qualificados por eles prestados cumprem os requisitos estabelecidos no Regulamento 910/2014; - Se necessário, tomar medidas face aos prestadores de serviços de confiança não qualificados estabelecidos no território do Estado-Membro que procede à designação, por meio de atividades de supervisão a posteriori, se lhe for alegado que os ditos prestadores ou os serviços de confiança por eles prestados não cumprem os requisitos estabelecidos no Regulamento 910/2014.
Validação de Selo Temporal	Declaração da entidade certificadora, que certifica a data e hora de criação, envio, ou receção de um documento eletrónico.
Prestador de Serviços de Confiança (PSC ou TSP)	Pessoa singular ou entidade legal que fornece um ou mais serviços de confiança, como prestador de serviços de confiança qualificados ou não qualificados.

1.6.2 Acrónimos

Acrónimo	Definição
ANSI	American National Standards Institute
BR	Baseline Requirements
CA	Certification Authority
CAA	Certification Authority Authorization
CAB	Conformity Assessment Body
CLMS	Certificates Lifecycle Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DL	Decree-law
DN	Distinguished Name
EAL	Evaluation Assurance Level
MAC	Message Authentication Codes
NCA	National Competent Authority
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object identifier
OVCP	Organizational Validation Certificate Policy

PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PSD2	Payment Services Directive 2
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QEVCP-w	Certificate policy for EU qualified website authentication certificates based on EVCP
QSealC	Qualified Electronic Seal Certificate
QSCD	Qualified electronic Signature/Seal Creation Device
QWAC	Qualified Website Authentication Certificate
SSCD	Secure Signature-Creation Device
TSA	Time-Stamping Authority (TSA)
TSP	Trust Service Provider

1.6.3 Referências Bibliográficas

Regulation EU No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on for electronic transactions in the internal market and repealing Directive 1999/93/EC

CA/Browser Forum, v1.8.6 – Baseline Requirements;

CA/Browser Forum, v1.8.0 – Guidelines for The Issuance and Management of Extended Validation Certificates;

Decreto-Lei nº 12/2021 – Assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno;

Despacho 154/2017 da Entidade Supervisora nacional, de 5 de dezembro – Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência;

Despacho 155/2017 da Entidade Supervisora nacional, de 5 de dezembro – Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário;

CWA 14167 - *Cryptographic Module for CSP Signing Operations - Protection Profile*;

CWA 14169:2004 - *Secure signature-creation devices "EAL 4+"*;

ETSI EN 319 401, v2.3.1 (2021-05) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

ETSI EN 319 411-1, v1.3.1 (2021-05) - Electronic Signatures and Infrastructures (ESI); Policy and security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

ETSI EN 319 411-2, V2.4.1 (2021-11) - 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 TS 119 412-1, v1.4.1 (2020-07) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

ETSI EN 319 412-1, v1.4.4 (2021-05) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

ETSI EN 319 412-2, v2.2.1 (2020-07) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

ETSI EN 319 412-3, V1.2.1 (2020-07) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;

ETSI EN 319 412-4, V1.2.1 (2021-11) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;

ETSI EN 319 412-5, v2.3.1 (2020-04) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;

ETSI EN 319 421, v1.1.1 (2016-03) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;

ETSI EN 319 422, v1.1.1 (2016-03) – Electronic Signatures and Infrastructure (ESI); Time-stamping protocol and time-stamp token profiles;

ETSI TS 119 495, v1.6.1 (2022-11) – Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366;

CEN/TS 419 241 v2014 – Security Requirements for Trustworthy Systems Supporting Server Signing;

FIPS 140-1. 1994, *Security Requirements for Cryptographic Modules*.

ISO/IEC 3166. 1997, *Codes for the representation of names and countries and their subdivisions*.

ITU-T *Recommendation* X.509. 1997, (1997 E*): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework*.

NIST FIPS PUB 180-1. 1995, *The Secure Hash Algorithm* (SHA-1). *National Institute of Standards and Technology, "Secure Hash Standard", U.S. Department of Commerce*.

RFC 1421. 1993, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.*

RFC 1422. 1993, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.*

RFC 1423. 1993, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.*

RFC 1424. 1993, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.*

RFC 6960. 2013, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

RFC 2986. 2000, PKCS #10: *Certification Request Syntax Specification, version* 1.7.

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

RFC 3279. 2002, *Algorithms and Identifiers for the Internet* X.509 *Public Key Infrastructure Certificate and Certificate Revocation List* (CRL) *Profile.*

RFC 3647. 2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

RFC 4510. 2006, *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.

RFC 4210. 2005, *Internet X.509 Public Key Infrastructure Certificate Management Protocol* (CMP).

RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List* (CRL) *Profile.*

RFC 6844. 2013, *DNS Certification Authority Authorization (CAA) Resource Record.*

RFC 6962. 2013, *Certificate Transparency.*

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

A Multicert S.A. é responsável pelas funções de repositório da PKI Multicert, publicando, entre outras, informação relativa às práticas adotadas e o estado dos certificados emitidos (CRL).

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

- Disponibilidade de serviços da plataforma de 99,9% (24x7), excluindo manutenções necessárias efetuadas em horário de menor utilização, garantindo-se durante o tempo da disponibilidade:
  - Mínimo de 99,990% de respostas a pedidos de obtenção da CRL;
  - Mínimo de 99,990% de respostas a pedidos do documento da DPC;
- Número máximo de pedidos de CRL: 50 pedidos/minuto;
- Número máximo de pedidos da DPC: 50 pedidos/minuto;
- Número médio de pedidos de CRL: 20 pedidos/minuto;
- Número médio de pedidos da DPC: 20 pedidos/minuto.

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

- CRL e DPC só podem ser alterados através de processos e procedimentos bem definidos;
- Plataforma tecnológica do repositório encontra-se devidamente protegida pelos mecanismos 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 Certificação

A Multicert S.A. mantém um repositório em ambiente web, permitindo que as *Relying Parties* efetuem pesquisas on-line relativas à DPC, PC, certificados de EC`s, revogação (CRL) e outra informação referente aos certificados, disponível em https://pki.multicert.com (e via URI`s incluídos nos próprios certificados).

São fornecidas declarações de conformidade quando solicitado através do email indicado na secção 1.5.2.

2.3 Periodicidade de Publicação

As atualizações a esta DPC e respetiva PC são publicadas até 7 dias após a sua aprovação pelo Grupo de Trabalho de Gestão, de acordo com a secção 9.12.

Os certificados das EC`s geridas pela Multicert são publicados logo que possível após a sua emissão.

As CRL`s emitidas pela EC Raiz da Multicert são publicadas logo que possível após a sua emissão.

As CRL`s emitidas pelas EC`s Subordinadas da Multicert são publicadas imediatamente após a sua emissão.

2.4 Controlo de Acesso aos Repositórios

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

3 Identificação e Autenticação

3.1 Atribuição de Nomes

A atribuição de nomes segue a seguinte convenção:

- Aos certificados de pessoa singular é atribuído o nome real do Subscritor/Titular (ou pseudónimo);
- Aos certificados de pessoa singular com associação de pessoa coletiva é atribuído o nome da pessoa singular no campo *Common Name*, e o nome da pessoa coletiva no campo *Organization*;
- Aos certificados de pessoa coletiva é atribuído o nome da entidade;
- Aos certificados de serviços é atribuído o nome qualificado do domínio e/ou o âmbito da sua utilização.

3.1.1 Tipos de Nomes

Os certificados das EC`s da PKI Multicert, assim como os certificados emitidos por estas, são identificados por um nome distinto (DN – Distinguished Name) de acordo com o standard X.500.

O nome distinto dos certificados está identificado no documento Lista de Perfis de Certificados (MULTICERT_PJ.ECRAIZ_428_pt) disponível em https://www.pki.multicert.com.

3.1.2 Necessidade de Nomes Significativos

A Multicert assegura, dentro das suas hierarquias de confiança:

- A não existência de certificados que, tendo o mesmo nome único, identificam entidades distintas;
- A relação entre o Subscritor/Titular e a organização a que pertence é a mesma que consta no certificado e é facilmente percetível e identificável pelos Humanos (com exceção dos certificados com pseudónimos).

3.1.3 Anonimato ou Pseudónimo de Subscritores/Titulares

Tipicamente, a Multicert não emite certificados com pseudónimos.

A Multicert pode emitir certificados com pseudónimo em casos específicos, sendo garantindo nesses casos que:

- O certificado contém o pseudónimo do Subscritor/Titular, claramente identificado como tal, sendo conservados os elementos que comprovam a verdadeira identidade dos requerentes Subscritores/Titulares de certificados com pseudónimo;
- Será comunicado à autoridade judiciária, sempre que esta o ordenar nos termos legalmente previstos, os dados relativos à identidade dos Subscritores/Titulares de certificados que sejam emitidos com pseudónimo seguindo-se, no aplicável, o regime do artigo 182.º do Código de Processo Penal.

3.1.4 Regras para Interpretação de Formato de Nomes

As regras utilizadas pela Multicert para interpretar o formato dos nomes seguem o estabelecido no RFC 5280[4], assegurando que todos os atributos DirectoryString dos campos "*issuer*" e "*subject*" do certificado são codificados no formato UTF8String, com exceção dos atributos "*country*" e "*serialnumber*" que são codificados no formato PrintableString.

3.1.5 Unicidade de Nomes

Os identificadores do tipo DN são únicos para cada Subscritor/Titular de certificado, emitido pela PKI Multicert, não induzindo em ambiguidades.

De acordo com os seus processos de emissão, a Multicert rejeita a emissão de certificados com o mesmo DN para Titulares distintos.

A unicidade de cada nome do "*subject*" num certificado é aplicada da seguinte forma:

- Certificado para assinatura eletrónica (qualificado ou não qualificado), autenticidade, confidencialidade – inclusão do nome do Subscritor/Titular (pessoa singular ou entidade legal) e adicionalmente o *serial number* do DN que é único. Quando o Subscritor/Titular está associado a uma entidade/organização, o nome da entidade também é incluído no DN.
- Certificado QWAC – inclusão do nome de domínio no certificado. A unicidade do nome de domínio é controlada pela entidade Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Reconhecimento, Autenticação, e Função de Marcas Registadas

As entidades requerentes de certificados têm que demonstrar que têm direito à utilização do nome requisitado, não podendo as designações usadas nos certificados emitidos pela PKI Multicert infringir os direitos de propriedade intelectual de outros indivíduos ou entidades.

No decorrer do procedimento de autenticação e identificação do Subscritor/Titular do certificado, previamente à emissão do mesmo, a entidade requerente do certificado tem que apresentar os documentos legais que demonstrem o direito à utilização do nome requisitado.

3.2 Validação de Identidade Inicial

Os certificados emitidos ao abrigo desta política estão sempre sujeitos a uma verificação meticulosa do indivíduo e / ou da organização para a qual o certificado será emitido.

Quando o certificado contém o campo *jurisdictionCountryName*, é feita uma verificação consultando uma Agência Incorporadora ou Agência de Registro listada no documento "Approved Incorporating Agencies" disponível em https://pki.multicert.com.

[4] cf. RFC 5280. 2008, InternetX.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile.

3.2.1 Método de Prova de Posse da Chave Privada

3.2.1.1 Assinatura (eSign)

O par de chaves e certificado é fornecido em token criptográfico (SmartCard ou token USB) com chip criptográfico, personalizado fisicamente para o Subscritor/Titular. A posse da chave privada é garantida pelo processo de emissão e personalização do token criptográfico, garantindo que:

1. O par de chaves é gerado no HSM criptográfico e inserido no token criptográfico, por comunicação direta segura e sem ficar registado em qualquer dispositivo;
2. O token criptográfico é personalizado para o Subscritor/Titular;
3. A chave pública é enviada à EC Multicert para emissão do correspondente certificado digital, sendo este também inserido no token criptográfico;
4. O token criptográfico é entregue presencialmente ou via correio;
5. O certificado é emitido no estado “suspenso”, sendo que para o ativar é disponibilizado um *link* ao Subscritor/Titular, através do qual, este se autentica com o certificado de Autenticação, que consta no token criptográfico. Ao fazer esta autenticação será enviado para o telemóvel do Subscritor/Titular, uma *password* temporária (OTP) que deverá ser introduzida na página de ativação do certificado, ficando este, assim que o processo seja concluído com sucesso, ativo e pronto a ser utilizado. Este último passo não é realizado nos certificados de assinatura não qualificados, autenticação e confidencialidade.

No caso dos certificados remotos, a chave privada é gerada e mantida num HSM. Neste caso, os passos anteriores não são realizados.

3.2.1.2 Selo Eletrónico (eSeal)

No caso de emissão de um certificado qualificado para Selo Eletrónico, são realizados os mesmos passos identificados na secção 3.2.1.1, exceto o passo 5 que não é realizado neste caso.

Para os certificados de Selo Eletrónico, existe também a opção de a chave ser gerada pela pessoa que solicita a emissão do certificado, desde que esteja devidamente autorizado pelo responsável legal da entidade, utilizando o seu próprio HSM. Neste caso:

1. A pessoa responsável e a entidade relevante são responsáveis pela chave gerada e pelo HSM usado para este propósito;
2. Deve ser fornecida à Multicert toda a documentação necessária assim como o CSR;
3. O certificado, após validação da documentação submetida, é devolvido à pessoa responsável.

O método usado para fazer prova da posse da chave privada tem que ser conforme com o standard PKCS#10.

3.2.1.3 Certificados Qualificados para Autenticação de Website

É garantido que o pedido de certificado inclui a chave privada correspondente à chave pública listada no certificado. O método para provar a posse da chave privada segue o standard PKCS#10.

3.2.1.4 Certificado de Serviços

A emissão de certificados para os serviços da PKI Multicert é efetuado por elementos que pertencem aos Grupos de Trabalho da PKI, aos quais são entregues os CSR`s gerados nos respetivos serviços.

O método para provar a posse da chave privada segue o standard PKCS#10.

3.2.2 Autenticação de Identidade da Organização

Para todos os certificados que incluem a identidade de uma organização, a validação dos dados da entidade legal é realizada de uma das seguintes formas:

- Utilizando documentos emitidos por entidades governamentais (Registo Comercial, Certidão Permanente, etc);
- Autenticação do formulário de pedido de certificado que contém os dados da organização, por uma entidade legal com poderes para tal ato (advogado, notário, solicitador);
- Uma base de dados de terceiros atualizada periodicamente.

No caso dos certificados SSL, a autoridade do Subscritor/Titular para solicitar um certificado em nome da organização é verificada de acordo com a secção 3.2.5 das *Baseline Requirements*.

Quando é incluído um nome de domínio no certificado, a Multicert autentica o direito da Organização para utilizar o nome de domínio como um *fully qualified domain name*. Nestes casos, é necessária confirmação do controlo do domínio, usando um dos métodos descritos na secção 3.2.2.2.

3.2.2.1 Método de Prova de Controlo de Endereço de Email

Quando é incluído um endereço de email nos atributos *Distinguished Name* ou *Subject Alternative Name* de um certificado digital, o Subscritor/Titular tem que provar que controla o endereço de email.

Para isso, a EC realiza um procedimento de desafio-resposta, que consiste em gerar um token e enviá-lo por email para o endereço de email a ser incluído no certificado. Para comprovar o controlo do endereço de email, o Subscritor/Titular clica no link que contém o token, que consta no email. A EC recebe a resposta e a prova de controlo de endereço de email é concluída com sucesso.

Este procedimento também é realizado para confirmar o endereço de email do Subscritor/Titular incluído no formulário de pedido de certificado (contacto de email do Subscritor).

3.2.2.2 Método de Validação de Controlo de Nome de Domínio / Endereço IP

A Multicert valida o direito de uso ou controlo por parte do requerente do nome de domínino / endereço IP, que será listado nos campos *Common Name* e *Subject Alternative Name* do certificado, utilizando pelo menos um dos seguintes procedimentos da secção 3.2.2.4 das Baseline Requirements:

Nome de Domínio	Endereço IP
Agreed-Upon Change to website – pelo requerente, através da colocação de um	Agreed-Upon Change to website – pelo requerente, através da colocação de um

token ou valor aleatório acordado, na diretoria "/.well-known/pki-validation", desempenhado de acordo com a secção 3.2.2.4.18 das Baseline Requirements.	token ou valor aleatório acordado, na diretoria "/.well-known/pki-validation", desempenhado de acordo com a secção 3.2.2.5.1
Email to DNS TXT Contact – confirmando o controlo por parte do requerente do FQDN através do envio de um valor aleatório por email para o contacto de email existente no registo DNS TXT associado ao Nome de Domínio Autorizado, e recebendo uma resposta utilizando o valor aleatório. Desempenhado de acordo com a secção 3.2.2.4.14 das Baseline Requirements.	Email to IP Address Contact – confirmando o controlo por parte do requerente do endereço IP através do envio de um valor aleatório por email e recebendo uma resposta de confirmação utilizando o valor aleatório. Desempenhado de acordo com a secção 3.2.2.5.2 das Baseline Requirements.
Phone Contact with Domain Contact – confirmando o controlo pelo requerente do FQDN através de chamada para o número de telefone do contacto do domínio e obtendo uma resposta de confirmação para validar o nome de domínio autorizado. Cada telefonema pode confirmar o controlo de vários nomes de domínio desde que o mesmo número de telefone do contacto de domínio esteja listado para cada um dos nomes de domíno autorizados a serem verificados, e desde que dêem uma resposta de confirmação para cada nome de domínio autorizado. Desempenhado de acordo com a secção 3.2.2.4.15 das Baseline Requirements.	Phone Contact with IP Address Contact – confirmando o controlo pelo requerente do endereço IP através de chamada para o número de telefone do contacto do endereço IP e obtendo uma resposta de confirmação para o pedido do requerente relativo ao endereço IP. Este método apenas pode ser usado quando o contacto do endereço IP está visível. Desempenhado de acordo com a secção 3.2.2.5.5 das Baseline Requirements.
DNS Change – pelo requerente, através da colocação de um token ou valor aleatório acordado, no DNS, CNAME, TXT ou CAA Record. Desempenhado de acordo com a secção 3.2.2.4.7 das Baseline Requirements.	
Constructed Email to Domain Contact – confirmando o controlo pelo requerente do FQDN através do envio de um email para 'admin', 'administrator', 'webmaster', 'hostmaster' ou 'postmaster' seguido de '@' seguido de um nome de domínio autorizado, incluindo no email um valor aleatório, e recebendo uma resposta de confirmação contendo o mesmo valor aleatório. Desempenhado de acordo com a secção 3.2.2.4.4 das Baseline Requirements.	

3.2.3 Autenticação de Identidade do Indivíduo

Quando um certificado inclui a identidade de uma pessoa singular, é realizada uma das seguintes validações de identidade:

1. Assinatura digital qualificada incluída no formulário de pedido de certificado, de acordo com o artigo 24.º, alínea 1.c), do Regulamento 910/2014;
2. Reconhecimento da identidade da pessoa singular por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador), de acordo com o artigo 24.º, alínea 1.a), do Regulamento 910/2014;
3. Através da presença física da pessoa singular nas instalações da ER, fazendo-se acompanhar pelo documento de identificação, de acordo com o artigo 24.º, alínea 1.a), do Regulamento 910/2014;
4. Através de sessão remota de videoconferência com a pessoa singular, de acordo com o Despacho 154/2017 da Entidade Supervisora Portuguesa, e do artigo 24.º, alínea 1.d), do Regulamento 910/2014;
5. Através do fornecedor de atributos Autenticação.gov, com Cartão de Cidadão ou Chave Móvel Digital, de acordo com o artigo 24.º, alínea 1.b), do Regulamento 910/2014.

Quando é incluído um endereço de email nos atributos *Distinguished Name* ou *Subject Alternative Name* do certificado digital, o Subscritor/Titular tem que fazer prova de controlo do email conforme descrito na secção 3.2.2.1.

Estas práticas estão em conformidade com os documentos ETSI EN 319 411-1 e ETSI EN 319 411-2 (quando se trata de um certificado qualificado).

3.2.4 Informação de Subscritor/Titular Não Verificada

Toda a informação fornecida pelo Subscritor/Titular é verificada.

3.2.5 Validação de Autoridade

A autoridade do indivíduo que solicita o certificado em nome do Subscritor, quando o Subscritor é uma Organização, é verificada de acordo com os seguintes métodos:

Certificados Qualificados de Autenticação de Website	Verificando os CAA Records se existirem (a identificação do domínio da EC Multicert nos CAA Records é 'multicert.com'). Verificado com base num contrato entre a EC e o Requerente, desde que o contrato seja assinado pelo número mínimo de pessoas com poderes para obrigar a entidade, ou por meio de um método de comunicação confiável após confirmação (utilizando um contato verificado através de uma agência governamental, uma base de dados de uma terceira parte, ou *attestation letter*) ou por meio de uma resolução corporativa. Os dados dos representantes da entidade são validados através de: assinatura digital qualificada do formulário de pedido de certificado; ou autenticação do formulário de

	pedido de certificado por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador); ou através de presença física nas instalações da ER fazendo-se acompanhar por documento de identificação; ou através de sessão remota de videoconferência.
Certificados Avançados de Assinatura	O Subscritor/Titular do certificado, ou no caso de uma entidade legal, com autorização da entidade legal. Os dados do Subscritor/Titular e dos representantes legais da entidade é validada através de: assinatura digital qualificada do formulário de pedido de certificado; ou autenticação do formulário de pedido de certificado por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador); ou através de presença física nas instalações da ER fazendo-se acompanhar por documento de identificação; ou através de sessão remota de videoconferência.
Certificados Qualificados de Assinatura (eSign)	O Subscritor/Titular do certificado, ou no caso de uma entidade legal, com autorização da entidade legal. Os dados do Subscritor/Titular e dos representantes legais da entidade é validada através de: assinatura digital qualificada do formulário de pedido de certificado; ou autenticação do formulário de pedido de certificado por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador); ou através de presença física nas instalações da ER fazendo-se acompanhar por documento de identificação; ou através de sessão remota de videoconferência.
Selos Eletrónicos Qualificados (eSeal)	Autorização pela entidade legal ou por um representante legal e autenticado. Os dados do subscritor e dos representantes legais da entidade é validada através de: assinatura digital qualificada do formulário de pedido de certificado; ou autenticação do formulário de pedido de certificado por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador); ou através de presença física nas instalações da ER fazendo-se acompanhar por documento de identificação; ou através de sessão remota de videoconferência.

3.2.6 Critérios para Interoperabilidade

Os certificados emitidos na PKI Multicert são emitidos debaixo de uma hierarquia de confiança.

3.3 Identificação e Autenticação para Pedidos de *Re-Key*

3.3.1 Identificação e Autenticação para Pedidos de Rotina de *Re-Key*

A Multicert requer ao Subscritor/Titular que use os mesmos detalhes de autenticação usados no pedido original de pedido de certificado.

3.3.2 Identificação e Autenticação para *Re-Key* após Revogação

Todos os pedidos após revogação são tratados como novas emissões de certificados, sujeitos ao mesmo procedimento de validação inicial.

3.4 Identificação e Autenticação para Pedido de Revogação

São consideradas formas de pedido de revogação autenticadas as seguintes:

- Pedido de revogação através da área de cliente – inserindo username e password;
- Pedido de revogação através da área de parceiro – apresentando certificado digital, username e password;
- Pedido de revogação através do Formulário Web de Pedido de Revogação – recebendo um token de revogação através de um meio de comunicação confiável;
- Pedido de revogação através do Formulário de Pedido de Revogação – assinado digitalmente, ou autenticado por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador), ou através de presença física nas instalações da ER pela pessoa que solicita a revogação;
- Pedido de revogação feito por elementos dos Grupo de Trabalho de Operação de Registo – apresentando certificado digital, username e password;
- Pela EC emissora – apresentando certificado digital, username e password;
- Pedido de revogação pela NCA (aplicável aos certificados PSD2) – submetido através de email acordado entre a NCA e o TSP.

Se o pedido for feito de outra forma, o processo de revogação de certificados emitidos pela PKI Multicert inicia-se com a suspensão, permitindo a validação adequada da autenticação do pedido.

4 Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Pedido de Certificado

O pedido de emissão de qualquer certificado à PKI Multicert inicia-se com o preenchimento de um formulário apropriado ao certificado pretendido. Os formulários para cada tipo de certificado encontram-se disponíveis na Loja Online da Multicert. Para cada tipo de certificado é indicada a informação necessária e o processo a seguir.

4.1.1 Quem Pode Submeter um Pedido de Certificado

Tanto o Subscritor/Titular como um indivíduo autorizado pelo Subscritor podem submeter um pedido de certificado. Os Subscritores são responsáveis pelos dados que o Subscritor ou um indivíduo autorizado pelo Subscritor submeta à Multicert.

O pedido de certificado deve ser acompanhado por um Formulário de Pedido de Certificado preenchido.

4.1.2 Processo de Registo e Responsabilidades

O processo de registo inclui os seguintes passos:

1. Certificados PSD2 e Selo Eletrónico Qualificado com QSCD nas instalações do cliente: geração do par de chaves e envio do CSR;
    1.1. Outros tipos de certificados: o par de chaves é gerado em QSCD/SSCD pela EC no momento de emissão do certificado, após serem realizadas todas as atividades seguintes.
2. Preenchimento do formulário de pedido de certificado;
3. Aceitação dos termos e condições de emissão do certificado;
4. Submissão do formulário de pedido de certificado;
5. Pagamento de custos aplicáveis;
6. Fornecimento de informação/documentação e/ou desempenhando as ações solicitadas pela ER de forma a permitir o processo de validação.

4.2 Processamento do Pedido de Certificado

4.2.1 Desempenhando Funções de Identificação e Autenticação

A Multicert, assim que rececione o formulário de pedido de emissão de certificado, bem como a informação necessária à emissão do pedido, procederá à validação de toda a informação disponibilizada a fim de verificar a autenticidade dos dados (ver secção 3.2).

Nos pedidos de certificados para Autenticação de Website, a Multicert efetua ainda verificações do CAA *records* relevantes no momento de submissão do pedido de certificado e imediatamente

antes da emissão do certificado. A EC atua de acordo com os CAA *records*, caso existam. O domínio de identificação da EC Multicert nos CAA *records* é 'multicert.com'[5].

4.2.2 Aprovação ou Rejeição de Pedidos de Certificado

A Multicert apenas aceita o pedido de certificado para emissão se todos os dados constantes no pedido forem autênticos, neste caso o pedido é aprovado.

No caso das informações constantes não forem verdadeiras ou inexistentes, a Multicert rejeita o pedido de emissão de certificado sendo o responsável pelo pedido devidamente informado.

4.2.3 Prazo de Processamento de Pedidos de Certificado

A Multicert dispõe de Service Level Agreements (SLAs), cuja informação se encontra disponível na Loja Online, para emissão de certificados. Contudo, a emissão dos certificados e o tempo que ocorre entre o pedido de certificado e a entrega do mesmo depende sobretudo da submissão completa da informação solicitada e da veracidade da mesma.

4.3 Emissão de Certificado

4.3.1 Ações da EC durante a Emissão do Certificado

Para qualquer certificado emitido pela PKI da Multicert, o pedido é sujeito a aprovação. Esta aprovação depende do tipo de certificado e da Entidade de Certificação em causa.

A emissão de certificado pela EC Raiz da Multicert requer uma cerimónia realizada por membros de vários grupos de trabalho que necessitam de autorizar operações individualmente, de forma a efetuar a operação de assinatura do certificado.

Para aprovação de certificado de utilizador final, o Grupo de Trabalho de Operação de Registo é responsável pela gestão e aprovação dos pedidos de certificados.

4.3.2 Notificação ao Subscritor/Titular pela EC Emissora do Certificado

O Subscritor/Titular ou o responsável pelo pedido de certificado será automaticamente notificado por email quando o certificado for emitido.

4.4 Aceitação do Certificado

4.4.1 Conduta que Constitui a Aceitação do Certificado

Os certificados qualificados de assinatura são emitidos no estado suspenso sendo que é da responsabilidade do Subscritor/Titular ativá-los mediante um conjunto de troca de informação entre o próprio e a Multicert.

[5] cf. RFC 6844. 2013, DNS Certification Authority Authorization (CAA) Resource Record

Os certificados são considerados aceites 7 dias após a sua emissão, ou antes se o certificado for usado quando exista evidência de que o Subscritor/Titular usou o certificado.

4.4.2 Publicação do Certificado pela EC

A Multicert publica todos os certificados de EC`s no seu repositório disponível em https://pki.multicert.com. A publicação de certificados de utilizador final é feita através da entrega do certificado ao Subscritor.

4.4.3 Notificação da Emissão do Certificado pela EC a Outras Entidades

Podem ser informados da emissão de certificado as ER`s Multicert ou parceiros/revendedores caso estejam envolvidos na solicitação inicial do certificado.

No caso dos certificados PSD2, pode ser notificada a NCA do país do Subscritor/Titular caso esta tenha indicado essa intenção previamente à Multicert.

4.5 Utilização do Certificado e Par de Chaves

4.5.1 Utilização do Certificado e Par de Chaves pelo Subscritor/Titular

Os Subscritores dos certificados apenas podem usar a chave privada dos seus certificados para a finalidade exclusiva a que a chave se destina (definida nos campos "*KeyUsage*" e "*Extended Key Usage*" do certificado) e sempre no âmbito do enquadramento legal. A utilização da chave é da exclusiva responsabilidade do Subscritor. Os termos e condições para emissão do certificado identificam as obrigações do Subscritor relativamente à proteção da chave privada e utilização aceitável.

4.5.2 Utilização do Certificado e Chave Pública pela *Relying Party*

As *Relying Parties* devem usar software em conformidade com os *standards* X.509 e devem apenas confiar no certificado se este não estiver expirado, suspendido ou revogado.

A Multicert fornece nesta DPC informação sobre os serviços apropriados disponíveis para verificar o estado de validade do certificado, tais como o OCSP e CRL.

4.6 Renovação de Certificado

A renovação de certificado refere-se à emissão de um novo certificado para o Subscritor, sem alteração da chave pública nem da informação contida no certificado.

4.6.1 Circunstâncias para a Renovação do Certificado

Um certificado pode ser substituído pela Multicert por sua iniciativa, ou pode ser renovado por iniciativa do Subscritor nas seguintes condições:

Certificados de Autenticação de Website podem ser renovados se:

- O certificado não está expirado nem revogado;
- O domínio mantém-se o mesmo. Se o(s) domínio(s) tiver(em) mudado, deve ser realizada uma nova validação do controlo de domínio conforme descrito na secção 3.2.2.2;
- A validade do certificado mantém-se a mesma do certificado anterior.

Para certificados QWAC PSD2, adicionalmente aplicam-se as seguintes condições:

- Os documentos e dados obtidos para verificar a informação do certificado, e a própria validação não tem mais que 398 dias;
- O certificado renovado pode ter uma validade diferente, desde que não ultrapasse o limite estabelecido na secção 6.3.2.

Quando a renovação do certificado não cumpre as condições acima, o processo é assumido como uma nova emissão.

4.6.2 Quem Pode Solicitar a Renovação

A EC Multicert pode iniciar a renovação de um certificado (substituição de certificado) por sua iniciativa, após notificar o Subscritor do certificado.
O Subscritor pode iniciar a renovação do certificado por sua iniciativa, apenas nas condições descritas na secção 4.6.1.

4.6.3 Processamento de Pedidos de Renovação de Certificado

Quando ocorre a renovação de um certificado, o par de chaves, data “Válido Até”, e os dados do *Distinguished Name* e *Subject Alternative Name* do certificado mantém-se os mesmos que a primeira emissão. Por esse motivo, a Multicert reutiliza por sua iniciativa a informação anteriormente verificada dentro dos limites de reutilização de informação descritos na secção 4.6.1.
Quando ocorre a substituição do certificado, os dados do *Distinguished Name* e/ou *Subject Alternative Name* podem mudar. Neste caso, são realizadas validações adicionais se necessário, sendo utilizado os métodos previsto na secção 3.2.

4.6.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

A Multicert notifica o Subscritor, tipicamente por email, em tempo razoável após a emissão do certificado, e pode usar qualquer mecanismo confiável para entregar o certificado ao Subscritor.

4.6.5 Conduta que Constitui a Aceitação do Certificado Renovado

Os certificados renovados são considerados aceites 7 dias após a sua entrega ou notificação da emissão do certificado ao Subscritor, ou quando exista evidência de que o Subscritor utilizou o certificado.

4.6.6 Publicação do Certificado Renovado pela EC

Ver secção 4.4.2.

4.6.7 Notificação do Certificado Emitido pela EC a Outras Entidades

Ver secção 4.4.3.

4.7 *Re-Key* de Certificado

Fazer *Re-Key* de um certificado consiste em criar um novo certificado com uma nova chave pública.

4.7.1 Circunstâncias para *Re-Key* de Certificado

Os pedidos de re-key são identificados e autenticados de acordo com o definido na secção 3.3.

4.7.2 Quem Pode Solicitar a Certificação de uma Nova Chave Pública

A Multicert pode aceitar um pedido de re-key de um certificado desde que seja proveniente do Subscritor do certificado ou de um Representante da Entidade/Organização, quando aplicável, ou pode proceder ao re-key de um certificado por sua iniciativa quando verifique que o certificado emitido não cumpre com os requisitos definidos no respetivo perfil de certificado ou DPC.

4.7.3 Processamento de Pedidos de *Re-Key* de Certificado

A Multicert pode solicitar informação adicional antes de processar um re-key e pode validar novamente o Subscritor, se necessário sujeito a nova verificação de quaisquer dados previamente validados.
O novo certificado emitido é enviado através de um meio de comunicação confiável previamente verificado.

4.7.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

A Multicert notifica o Subscritor num prazo razoável após a emissão do certificado.

4.7.5 Conduta que Constitui a Aceitação do Certificado para o qual foi feito *Re-Key*

Os certificados emitidos são considerados aceites 7 dias após ser feito *re-key* do certificado, ou antes caso exista evidência de utilização do certificado pelo Subscritor.

4.7.6 Publicação do Certificado pela EC para o qual foi feito Re-Key

A Multicert publica os certificados para os quais foi feito *re-key*, entregando-os ao Subscritor.

4.7.7 Notificação de Emissão de Certificado pela EC a Outras Entidades

Sem Estipulação.

4.8 Modificação de Certificado

A modificação de certificado refere-se à emissão de um novo certificado devido a alterações na informação do certificado que não a chave pública do Subscritor.

4.8.1 Circunstâncias para a Modificação de Certificado

Um certificado pode ser modificado por iniciativa da Multicert quando se verifica que este não cumpre com os requisitos definidos no respetivo perfil de certificado ou DPC.
Os certificados podem ser modificados se:

- O certificado não está expirado nem revogado.

4.8.2 Quem Pode Solicitar a Modificação de Certificado

A Multicert pode iniciar a modificação de um certificado por sua iniciativa, após notificar o Subscritor do certificado.

4.8.3 Processamento de Pedidos de Modificação de Certificado

Quando a modificação do certificado incide sobre os dados constantes no *Distinguished Name* e/ou *Subject Alternative Name*, a Multicert realiza validações adicionais dos dados a serem alterados. Quando são efetuadas outras alterações que não os dados do *Distinguished Name* e/ou *Subject Alternative Name*, a Multicert reutiliza a informação do pedido de certificado inicial. A validade do certificado modificado nunca é superior à validade do certificado inicial. A validade do certificado modificado nunca é superior à validade do certificado inicial.

4.8.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

A Multicert notifica o Subscritor, tipicamente por email, em tempo razoável após a emissão do certificado, e pode usar qualquer mecanismo confiável para entregar o certificado ao Subscritor.

4.8.5 Conduta que Constitui Aceitação de Certificado Modificado

Os certificados modificados são considerados aceites 7 dias após a sua entrega ou notificação da emissão do certificado ao Subscritor, ou quando exista evidência de que o Subscritor utilizou o certificado.

4.8.6 Publicação do Certificado Modificado pela EC

Ver secção 4.4.2.

4.8.7 Notificação de Emissão de Certificado pela EC a Outras Entidades

Ver secção 4.4.3.

4.9 Revogação e Suspensão de Certificado

4.9.1 Motivos para Revogação

A revogação ou suspensão de certificados são ações através das quais o certificado perde a sua validade antes do término do período de validade, perdendo a sua operacionalidade.

Certificados no estado suspenso podem ser revertidos para o estado ativo. Certificados no estado revogado não podem ser revertidos para o estado ativo.

Se uma das seguintes razões ocorrer, o certificado é revogado dentro de 24 horas:

- O Subscritor solicita à EC a revogação do certificado, através da submissão de um formulário de pedido de revogação;
- O Subscritor notifica a EC de que o pedido original de certificado não foi autorizado e não concede autorização com efeitos retroativos;
- A chave privada e/ou a password de acesso à chave privada (i.e. PIN) foi comprometido ou existe suspeita de comprometimento;
- A chave privada foi perdida;
- A EC tem conhecimento de um método demonstrado ou comprovado que pode facilmente computar a chave privada do Subscritor com base na chave pública do certificado;
- A EC obtém evidência de que a validação da autorização ou controlo do domínio de qualquer nome de domínio qualificado ou endereço IP do certificado não deve ser considerada.

Se uma das seguintes razões ocorrer, o certificado é revogado dentro de 5 dias:

- O certificado foi usado para finalidade não autorizadas;
- A EC é informada de uma alteração significativa na informação contida no certificado;
- A EC determina ou tem conhecimento de que qualquer informação do certificado é imprecisa;
- A EC tem conhecimento de que o Subscritor violou um ou mais obrigações estipuladas nos termos e condições de emissão do certificado digital;

- A EC tem conhecimento de que o certificado não foi emitido de acordo com os requisitos da EC previstos na DPC, PC ou requisitos normativos aplicáveis;
- O algoritmo e tamanho de chave do certificado, ou a geração e verificação da qualidade dos parâmetros da chave pública já não estão em conformidade com a ETSI TS 119 312;
- A EC tem conhecimento de quaisquer circunstâncias que indiquem que a utilização do nome de domínio qualificado ou endereço IP do certificado já não são legalmente permitidos (ex: foi revogado pelo tribunal o direito de uso do nome de domínio ao *Domain Name Registrant*, foi rescindido um licenciamento ou contrato de serviços relevante entre o *Domain Name Registrant* e o Subscritor, ou o *Domain Name Registrant* falhou a renovação do nome de domínio);
- A EC tem conhecimento de um método demonstrado ou comprovado que expõe ao comprometimento da chave privada do Subscritor, foram desenvolvidos métodos que podem calcular facilmente a chave privada com base na chave pública (como uma chave fraca Debian, ou se houver evidência de que o método específico usado para gerar a chave privada tinha falhas;
- Quando aplicável, se o token/smartcard criptográfico onde a chave privada está armazenada tenha sido perdido, destruído ou deteriorado.

Se uma das seguintes razões ocorrer, o certificado pode ser revogado pela EC:

- A EC é notificada devido a uma resolução legal ou administrativa;
- A EC tem conhecimento de que o certificado foi usado para atividades ilícitas;
- A EC cessa operações e não encontra outra EC que forneça suporte à revogação dos certificados.

Se uma das seguintes razões ocorrer, o certificado PSD2 pode ser revogado a pedido da NCA:

- A NCA retira um ou mais papéis ao PSP, que estavam incluídos no certificado;
- A NCA retira a autorização PSD2 ao PSP que solicitou o certificado.

Se uma das seguintes razões ocorrer, a EC Subordinada é revogada dentro de7 dias:

- A EC Subordinada solicita a revogação por escrito;
- A EC Subordinada notifica a EC Emissora de que o pedido de certificado original não foi autorizado e não concede autorização com efeitos retroativos;
- A EC Emissora obtém evidência de que a chave privada da EC Subordinada correspondente à chave pública no certificado sofreu um comprometimento ou já não está em conformidade com a ETSI TS 119 312;
- A EC Emissora obtém evidência de que o certificado foi usado para finalidades não autorizadas;
- A EC Emissora tem conhecimento de que o certificado não foi emitido de acordo com ou a EC Subordinada não cumpriu com os requisitos Baseline Requirements ou PC aplicável ou DPC, no caso dos certificados QWAC;
- A EC Emissora determina que qualquer informação constante no certificado é imprecisa ou enganadora;
- A EC Emissora ou a EC Subordinada cessa operações por qualquer razão e não tem acordos com outra EC para o fornecimento de suporte à revogação do certificado;
- É requerida revogação pela DPC e/ou PC da EC Emissora.

4.9.2 Quem Pode Solicitar Revogação

O pedido de revogação pode ser feito por um dos seguintes elementos:

- Pelo cliente/subscritor ou um representante;
- Pela entidade/organização que solicitou o certificado;
- Por um elemento do Grupo de Trabalho de Operação de Registo da PKI Multicert ou pela EC Emissora, quando tenha conhecimento de que os dados incluídos no certificado não correspondem à verdade ou não são detidos pelo Subscritor ou quando ocorra uma das razões de revogação definidas na secção 4.9.1;
- Pela NCA, quando se trata de certificados PSD2, devido a uma razão devidamente fundamentada tal como a informação contida no certificado deixe de ser válida.

4.9.3 Procedimento para o Pedido de Revogação

O pedido de revogação pode ser apresentado de uma das seguintes formas:

- On-line, usando o Formulário Web de Pedido de Revogação, em que o estado do certificado será alterado para REVOGADO:
  - https://www.multicert.com/3ws/certRevocationForm?lang=pt_PT
- Através do envio direto do Formulário de Pedido de Revogação, disponível pela Multicert no seu *site*, devidamente preenchido e acompanhado da documentação solicitada para esta finalidade;
- Utilizando os serviços online da Área de Cliente ou Área de Parceiro, não sendo necessário submeter qualquer documentação;
- Se a NCA solicitar a revogação (apenas aplicável aos certificados PSD2): a NCA envia um email solicitando a revogação do certificado, submetendo o formulário de pedido de revogação e indicando qual o método de validação da autenticidade do pedido que pretende usar, dos métodos descritos na secção 6.2.3 da ETSI TS 119 495:
  - Segredo Partilhado – a EC irá contactar a NCA, por telefone, para partilhar o segredo com a NCA. A NCA deve enviar um email contendo o segredo partilhado e submetendo o formulário de pedido de revogação do certificado;
  - Assinatura Digital – a NCA envia um email contendo o formulário de pedido de revogação do certificado assinado digitalmente com certificado qualificado. O certificado qualificado deve ser um dos seguintes: selo qualificado contendo o nome da NCA no campo *Organization*, ou uma assinatura qualificada com o nome da pessoa na NCA que solicita a revogação do certificado (neste caso, o certificado deve conter o nome da NCA no campo *Organization*).

4.9.4 Período de Carência do Pedido de Revogação

O período de carência do pedido de revogação é o tempo disponível para o Subscritor tomar as ações necessárias para pedir a revogação de um certificado sobre o qual exista suspeita de comprometimento da chave, utilização de uma chave fraca ou descoberta de informação imprecisa contida no certificado.

Nesta situação, o Subscritor deve pedir a revogação no prazo de 24 horas após a sua deteção.

4.9.5 Tempo de Processamento do Pedido de Revogação pela EC

Quando o pedido de revogação é feito pelo Subscritor ou pessoa responsável pela Entidade/Organização, através de formulário de pedido de revogação escrito, o Grupo de Trabalho de Operação de Registo tem 24 horas, após receber o formulário de pedido de revogação, para o processar e revogar o certificado. Se o pedido de revogação é feito através de um meio autenticado, o processamento da revogação é imediato. A Multicert garante a publicação do novo estado do certificado dentro dos seguintes prazos:

- No caso da CRL dentro do período indicado na secção 4.9.7.
- Imediatamente através de OCSP.

4.9.6 Requisito de Verificação da Revogação pelas Relying Parties

Antes de confiar na informação listada num certificado, a Relying Party deve validar a adequação do certificado para a finalidade pretendida e garantir que o certificado é válido. Para verificar o estado do certificado, as Relying Parties necessitam consultar as respostas OCSP ou CRL identificadas em cada certificado.
A informação de estado do certificado é consistente entre a CRL e OCSP. A informação de alteração de estado no OCSP após a revogação é atualizada imediatamente. A alteração de estado na CRL contém a mesma informação de revogação que consta no OCSP, no entanto a publicação de uma nova CRL só acontece dentro da periodicidade definida na secção 4.9.7, pelo que em caso de divergência deve ser considerada a informação disponibilizada no OCSP.

4.9.7 Frequência de Emissão de CRL

As Entidades de Certificação Multicert autorizadas a emitir certificados para utilizadores finais emitem CRL`s diariamente, sendo emitidas Delta CRL`s a cada 12 horas.

No caso da EC Raíz, a CRL é emitida a cada 12 meses ou dentro de 24 horas se for revogada uma EC Subordinada.

4.9.8 Latência Máxima para CRLs

As CRL`s de certificados emitidos para utilizadores finais são publicadas automaticamente no repositório online, dentro de um prazo comercialmente razoável após a sua geração, tipicamente dentro de minutos após a sua geração.
Quando são emitidas CRL`s da EC Raiz devido à revogação de EC Subordinada, a CRL é publicada dentro de 24 horas após a sua emissão. As CRL`s regularmente agendadas são publicadas antes do campo nextUpdate da CRL anteriormente emitida para o mesmo âmbito.

4.9.9 Disponibilidade de Verificação de Estado/Revogação *On-Line*

A Multicert dispõe de um serviço de resposta para validação *online* do estado de certificado, com uma disponibilidade correspondente a 99,9%.

O serviço OCSP fornece uma validação em tempo real do estado do certificado.

As respostas OCSP estão em conformidade com o RFC 6960 ou RFC 5019. As respostas OCSP são assinadas por um *responder* OCSP cujo certificado é assinado pela EC que emitiu o certificado sobre o qual se está a verificar o estado de revogação.

4.9.10 Requisitos de Verificação de Revogação *On-Line*

A *Relying Party* deve confirmar a validade do certificado de acordo com a secção 4.9.6 antes de confiar no certificado.

Os OCSP *responders* que recebam um pedido de estado de um certificado que ainda não foi emitido, não respondem com o estado "*good*" para tal certificado.

4.9.11 Outras Formas Disponíveis de Anunciar Revogação

Sem Estipulação.

4.9.12 Requisitos Especiais Relacionados com o Comprometimento de Chave

A Multicert e Entidades de Registo usam métodos comercialmente razoáveis para informar os Subscritores de que a sua chave privada pode ter sido comprometida.

A comunicação de uma chave privada comprometida deve ser efetuada através do envio de email para os contactos indicados na secção 1.5.2.

Podem ser usados os seguintes métodos para demonstrar o comprometimento de uma chave privada:

- Assinando um CSR com a chave privada comprometida, contendo uma entrada *Common Name* "Proof of Key Compromise for Multicert";
- Enviando a chave privada comprometida.

4.9.13 Motivos para Suspensão

É permitida a suspensão de certificados, exceto no caso dos certificados QWAC.

A suspensão do certificado pode ser usada quando o Subscritor, o Responsável pela Entidade/Organização (quando aplicável), ou a Entidade de Registo pretendem desabilitar o certificado temporariamente. Pode levar a isso situações como a perda temporária do certificado, ou a saída temporária do Subscritor da Entidade/Organização. Contrariamente à revogação do certificado, a suspensão permite que o estado do certificado seja alterado para ativo ou revogado.

4.9.14 Quem Pode Solicitar Suspensão

O pedido de suspensão pode ser efetuado por um dos seguintes elementos:

- Pelo Cliente/Subscritor ou um Representante;
- Pela Entidade/Organização que solicitou o certificado;
- Por um elemento do Grupo de Trabalho de Operação de Registo da PKI Multicert ou pela EC.

4.9.15 Procedimento para o Pedido de Suspensão

O pedido de suspensão pode ser apresentado de uma das seguintes formas:

- On-line, utilizando o Formulário Web de Pedido de Suspensão (não aplicável aos certificados SSL), em que o estado do certificado é alterado para suspenso: https://www.multicert.com/3ws/certSuspensionForm.
- Utilizando os serviços online da Área de Cliente ou Área de Parceiro, não sendo necessário submeter documentação.

4.9.16 Limites do Período de Suspensão

No caso dos certificados digitais qualificados (eSign ou eSeal), se o certificado for suspenso:

- Através da área de cliente – o Subscritor tem 3 dias para ativar o certificado, caso contrário o certificado será revogado;
- Através da área de parceiro ou através do Formulário Web de Pedido de Suspensão – o Subscritor tem 6 dias para submeter o pedido de revogação, caso contrário o certificado será ativado;
- Através de outros meios – o Subscritor deve submeter o pedido à ER para ativar ou revogar o certificado. Se o Subscritor não submeter o pedido de revogação, o certificado poderá ficar suspenso até ao final da sua validade.

No caso dos certificados não qualificados, o Subscritor deve submeter o pedido à ER para ativar ou revogar o certificado. Se o Subscritor não submeter o pedido de revogação, o certificado poderá ficar suspenso até ao final da sua validade.

4.10 Serviços de Estado de Certificado

4.10.1 Características Operacionais

O estado de certificados emitidos está disponível publicamente utilizando CRL`s, Delta CRL´s e o serviço OCSP.

Se um certificado for revogado, este mantém-se na CRL após a sua data de expiração.

4.10.2 Disponibilidade de Serviço

O serviço de estado de certificado está disponível 24 horas por dia, 7 dias por semana.

4.10.3 Funcionalidades Opcionais

Sem Estipulação.

4.11 Fim de Subscrição

A operacionalidade do certificado terminará quando ocorra uma das seguintes circunstâncias:

- Revogação do certificado;
- Expiração do período de validade do certificado;
- O contrato do Subscritor aplicável expira sem que seja renovado.

4.12 Custódia e Recuperação de Chaves

4.12.1 Política e Práticas de Custódia e Recuperação de Chaves

A PKI Multicert não faz custódia de chaves de certificados para utilizador final.

A PKI Multicert pode fazer custódia de chaves para chaves privadas de EC`s, neste caso é planeada e realizada uma cerimónia pelos membros dos grupos de trabalho necessários, de acordo com os artefactos necessários para esta operação. As chaves privadas das EC`s da Multicert são sujeitas aos controlos técnicos descritos na secção 6.2.3.

4.12.2 Política e Práticas de Encapsulamento e Recuperação de Chave de Sessão

Sem Estipulação.

5 Controlos de Segurança Física, Gestão e Operacionais

A Multicert implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes nesta DPC. Esta secção descreve sucintamente os aspetos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos Subscritores/Titulares, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança nos certificados, pois qualquer falha de segurança pode comprometer as operações da EC.

5.1 Controlos de Segurança Física

5.1.1 Localização Física e Tipo de Construção

As instalações da PKI Multicert são desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas de 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 das EC`s da PKI Multicert são realizadas numa sala em 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 características:

a) Paredes em alvenaria, betão ou tijolo;

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

c) Inexistência de janelas;

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

Adicionalmente, as seguintes condições de segurança são garantidas no ambiente PKI Multicert:

- Perímetros de segurança claramente definidos;
- Paredes, chão e teto em alvenaria, betão ou tijolo, 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;

- O 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

Os sistemas da PKI 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.

As atividades operacionais sensíveis das EC`s, 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. Os acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias.

O acesso ao cartão de identificação obriga a um duplo controlo de autenticação de acesso individual. Ao pessoal não acompanhado, incluindo colaboradores ou visitantes não autenticados, não é permitida a sua entrada e permanência em áreas de segurança. A não ser que todo o pessoal que circule dentro destas áreas de segurança seja garantidamente reconhecido por todos, é obrigatório o uso do respetivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respetivo cartão de acesso visível.

O acesso à zona mais restrita de alta segurança requer, no mínimo, 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. O acesso à zona mais restrita de alta segurança, assim como ao hardware criptográfico e aos tokens físicos seguros 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 da Multicert possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de:

- Fornecimento de energia elétrica ininterrupta com a potência suficiente para manter autonomamente a disponibilidade do serviço durante períodos de falta de abastecimento da rede pública. O sistema garante a proteção dos equipamentos face a flutuações elétricas que os possam danificar (a alternativa à rede pública é garantida por unidades de alimentação ininterrupta e baterias, bem como 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. A desconformidade dos parâmetros de temperatura/humidade despoleta o envio de alarmes para as equipas de manutenção e para a Central de Segurança.

5.1.4 Exposição à Água

As zonas de alta segurança têm instalados os mecanismos devidos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da PKI Multicert.

5.1.5 Prevenção e Proteção contra Incêndio

O ambiente seguro 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:

- Estão instalados nos vários níveis físicos de segurança, sistemas de deteção e alarme de incêndio;
- Estão disponíveis equipamentos fixos e móveis de extinção de incêndios, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;
- Existem procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6 Armazenamento de *Media*

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 estão implementados mecanismos de proteção contra acidentes (e.g., causados por água ou fogo).

Quando, para efeitos de arquivo de cópias de segurança, é transportada informação sensível da zona de alta segurança para o ambiente externo, o processo é executado sob supervisão de pelo menos 2 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 impliquem 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 de 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 (formatação do disco rígido, reset do hardware criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7 Eliminação de Resíduos

Os documentos e materiais em papel que contenham informação sensível são triturados antes da sua eliminação.

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível (através de formatação “segura” de baixo nível ou destruição física), antes dos mesmos serem eliminados. Os equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Os outros

equipamentos de armazenamento (como discos rígidos ou tapes) são devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

5.1.8 *Backup* em Instalações Externas

Todas as cópias de segurança são guardadas 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 Controlos Procedimentais

A atividade de uma Entidade Certificadora depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente:

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

Por este motivo, nesta secção descrevem-se os papéis de confiança e responsabilidades associadas a cada um desses papéis.

5.2.1 Grupos de Trabalho

Definem-se como pessoas autenticadas todos os colaboradores, fornecedores e consultores que tenham acesso ou que controlem operações criptográficas ou de autenticação.

A Multicert estabeleceu que os papéis de confiança fossem agrupados em 8 categorias diferentes (que correspondem a 6 Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticadas, pertencentes a diferentes Grupos de Trabalho.

Não estão autorizadas entradas no “Ambiente de Produção” sem a presença mínima de dois elementos, pertencente a Grupos de Trabalho distintos (com exceção do Grupo de Trabalho de Custódia que não tem permissão para aceder a este ambiente).

Como medida adicional de segurança, a Multicert considera relevante, mas não obrigatória, a presença em todas as intervenções de um elemento de Auditoria.

5.2.1.1 Grupo de Trabalho de Operação

É responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade das EC`s.

5.2.1.2 Grupo de Trabalho de Autenticação

É responsável por assegurar a gestão, salvaguarda e disponibilidade de passwords e tokens de autorização (não pessoais), e a definição, atualização, e proposta de políticas das EC`s ao Grupo de Trabalho de Gestão.

5.2.1.3 Grupo de Trabalho de Auditoria

É responsável por efetuar a auditoria interna de todas as ações relevantes e necessárias para assegurar a operacionalidade das EC`s.

5.2.1.4 Grupo de Trabalho de Custódia

É responsável pela custódia de alguns artefactos sensíveis (tokens de autenticação, entre outros), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições. Note-se que, no sentido de melhorar os níveis de segurança, operacionalidade e continuidade de negócio das EC`s, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de artefactos. Este grupo faz uso dos vários ambientes seguros disponibilizados para a guarda deste tipo de itens.

5.2.1.5 Grupo de Trabalho de Operação de Registo

É responsável por validar a documentação relacionada com o pedido de certificado, assegurar a emissão, renovação, suspensão e revogação de certificados.

5.2.1.6 Grupo de Trabalho de Administração de Sistemas

É responsável pela instalação, configuração e manutenção dos sistemas da PKI (hardware e software). É também responsável pela consolidação e análise da monitorização dos pontos de controlo de segurança de todos os recursos utilizados na PKI da MULTICERT, que podem dar origem a eventos, alarmes e incidentes.

5.2.1.7 Grupo de Trabalho de Gestão

É o órgão de decisão da PKI Multicert.

A missão do Grupo de Trabalho de Gestão assenta principalmente na tomada de decisões importantes e críticas ao bom funcionamento das EC`s da PKI Multicert, realçando-se a revisão e aprovação de todos os documentos e políticas das EC`s propostas pelo Grupo de Trabalho de Autenticação. O Grupo de Trabalho de Gestão tem ainda como missão a nomeação e/ou destituição dos membros dos restantes grupos e a guarda de alguns artefactos sensíveis (tokens de autenticação, entre outros).

5.2.1.8 Grupo de Trabalho de Manutenção

É responsável por assegurar o acompanhamento e supervisão de ações de manutenção e limpeza das salas do CPD.

5.2.2 Número de Pessoas Exigidas por Tarefa

Existem procedimentos de controlo rigorosos que obrigam à divisão de responsabilidades baseadas nas especificidades de cada Grupo de Trabalho, e de modo a garantir que tarefas sensíveis apenas podem ser executadas por um conjunto múltiplo de pessoas autenticadas.

Os procedimentos de controlo interno foram elaborados de modo a garantir um mínimo de 2 indivíduos autenticados para se ter acesso físico ou lógico aos equipamentos de segurança. O acesso ao hardware criptográfico das EC`s segue procedimentos estritos envolvendo múltiplos indivíduos autorizados a aceder-lhe durante o seu ciclo de vida, desde a receção e inspeção até à destruição física e/ou lógica do hardware. Após a ativação de um módulo com chaves

operacionais, são utilizados controlos adicionais de acesso de modo a garantir que os acessos físicos e lógicos ao hardware só são possíveis com 2 ou mais indivíduos autenticados. Indivíduos com acesso físico aos módulos, não detêm as chaves de ativação e vice-versa.

5.2.3 Identificação e Autenticação por Função

É da responsabilidade do Grupo de Trabalho de Gestão nomear os elementos que fazem parte dos restantes grupos.

O resultado desta nomeação é descrito no documento Política de Recursos Humanos da PKI Multicert, que é distribuído por todos os elementos.

Com base neste documento, são configurados os acessos aos ambientes e sistemas relacionados com a PKI Multicert.

5.2.4 Funções que Requerem Separação de Responsabilidades

A matriz seguinte define as incompatibilidades (assinaladas por ✘) entre a pertença ao grupo identificado nas colunas e a pertença ao grupo identificado nas linhas, no contexto da PKI Multicert:

Se pertence ao Grupo ... / Pode pertencer ao Grupo?	Administração de Sistemas	Operação	Autenticação	Operação de Registo	Auditoria	Custódia	Gestão	Manutenção
Administração de Sistemas			✘	✘	✘	✘	✘	
Operação			✘		✘	✘	✘	
Autenticação	✘	✘		✘	✘	✘	✘	✘
Operação de Registo	✘	✘	✘		✘	✘	✘	✘
Auditoria	✘	✘	✘	✘		✘	✘	✘
Custódia	✘	✘	✘	✘	✘		✘	✘
Gestão	✘	✘	✘	✘	✘	✘		✘
Manutenção			✘	✘	✘	✘	✘	

5.3 Controlos de Segurança Pessoal

A admissão de pessoal com funções de confiança nos Grupos de Trabalho é apenas possível se forem cumpridas as seguintes condições:

- Ser formalmente nomeado para a função;
- Ter recebido treino adequado para a função;
- Fazer prova da sua identidade, usando documentação emitida por fontes fiáveis;
- Fazer prova de não possuir antecedentes criminais;
- Fazer prova de que possui as qualificações e experiência exigidas pela entidade ou grupo que efetuou a sua nomeação formal;
- Comprometer-se (formalmente) a não revelar (salvo com autorização expressa dos representantes legais da entidade que detém as EC`s) qualquer informação sobre as EC`s, seu funcionamento, sobre os ambientes e recursos humanos ao seu serviço e sobre os titulares dos certificados digitais por esta emitidos;
- Comprometer-se (formalmente) a desempenhar as funções para as quais foi nomeado e a não assumir responsabilidades que possam colocar problemas éticos ou deontológicos à sua execução. Nesse sentido, é necessário que declare não só conhecer os termos e condições para o desempenho das respetivas funções, como também a sua capacidade e disponibilidade para o fazer.

5.3.1 Requisitos relativos a Qualificações, Experiência e Autorização

A admissão de novos membros nos Grupos de Trabalho é apenas possível se apresentarem provas de conhecimento, qualificações e experiência necessárias para a realização das tarefas dos Grupos de Trabalho.

5.3.2 Procedimentos de Verificação de Antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer uma das funções de confiança. A verificação de antecedentes inclui:

- Confirmação de identidade, usando documentação emitida por fontes fiáveis; e
- Investigação de registos criminais.

5.3.3 Requisitos de Formação

É ministrado aos membros dos Grupos de Trabalho formação e treino adequado de modo a realizarem as suas tarefas, satisfatória e competentemente.

Os elementos dos Grupos de Trabalho estão sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

a) Certificação digital e Infraestruturas de Chave Pública;
b) Conceitos gerais sobre segurança da informação;
c) Formação específica para o seu papel dentro do Grupo de Trabalho;
d) Funcionamento do software e/ou hardware usado pela EC;
e) Política de Certificado e Declaração de Práticas de Certificação;
f) Recuperação de desastres;

g) Procedimentos para a continuidade da atividade; e

h) Aspetos legais básicos relativos à prestação de serviços de certificação.

5.3.4 Frequência e Requisitos para Atualização de Formação

São realizadas ações de formação e treino, no mínimo, a cada 12 meses.

Sempre que necessário é ministrado treino e formação complementar aos membros dos Grupos de Trabalho, de modo a garantir o nível pretendido de profissionalismo para a execução competente e satisfatória das suas responsabilidades. Em particular:

- Sempre que existam alterações tecnológicas, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto às EC`s;
- Sempre que sejam introduzidas alterações na Política de Certificado ou Declaração de Práticas de Certificação são realizadas sessões de atualização de formação aos elementos das EC`s.

5.3.5 Frequência e Sequência da Rotação de Funções

Sem Estipulação.

5.3.6 Sanções para Ações Não Autorizadas

Consideram-se ações não autorizadas todas as que desrespeitem a Declaração de Práticas de Certificação e a Política de Certificado, quer sejam realizadas de forma deliberada ou sejam ocasionadas por negligência.

São aplicadas sanções de acordo com as regras de trabalho, legislação nacional e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

5.3.7 Requisitos para Prestadores de Serviços Independentes

Consultores ou prestadores de serviços independentes têm permissão de acesso à zona de alta segurança desde que estejam sempre autorizados, acompanhados e diretamente supervisionados por elementos pertencentes aos Grupos de Trabalho e após tomada de conhecimento e aceitação da Declaração de Confidencialidade.

5.3.8 Documentação Fornecida ao Pessoal

É disponibilizado aos membros dos Grupos de Trabalho toda a informação adequada para que estes possam realizar as suas tarefas, de modo competente e satisfatório.

5.4 Procedimentos de Registo de Auditoria

5.4.1 Tipos de Eventos Registados

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

- Pedido, emissão, renovação, reemissão e revogação de certificados;
- Publicação de CRL;
- Eventos relacionados com segurança, incluindo:
  - Tentativas de acesso (com e sem sucesso) a recursos sensíveis das EC`s;
  - 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 seguinte informação:

- 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 de Processamento 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 de Registos de Auditoria

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

5.4.4 Proteção de Registos de Auditoria

Os registos são apenas analisados por elementos autorizados pertencentes aos Grupos de Trabalho.

Os registos são 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.

5.4.5 Procedimentos de Cópia de Segurança de Registos de Auditoria

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade.

5.4.6 Sistema de Recolha de Registos (Interno vs. Externo)

Os registos são recolhidos em simultâneo, interna e externamente aos sistemas das EC`s.

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 Avaliações de Vulnerabilidades

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

5.5 Arquivo de Registos

5.5.1 Tipos de Registos Arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.4.1), assim como a 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 por um período de tempo de 7 anos após a data de expiração do certificado a quem digam respeito.

5.5.3 Proteção do Arquivo

O arquivo:

- É protegido para que apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao seu conteúdo;
- É protegido contra qualquer modificação ou tentativa de remoção;
- É protegido contra a deterioração do *media* onde é guardado, através de migração periódica para *media* novo;
- É protegido contra a obsolescência do hardware, sistemas operativos e outro software, pela conservação do hardware, sistemas operativos e outro software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal; e

- É guardado de modo seguro em ambientes externos.

5.5.4 Procedimentos para Cópia de Segurança do Arquivo

São efetuadas cópias de segurança dos arquivos, de modo incremental ou total e guardadas em dispositivos apropriados.

5.5.5 Requisitos para Validação Cronológica de Registos

Algumas das entradas dos arquivos contêm informação de data e hora baseadas em fonte de tempo segura.

5.5.6 Sistema de Recolha de Arquivo (Interno ou Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7 Procedimentos para Obter e Verificar Informação de Arquivo

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos, sendo a sua integridade verificada através do seu restauro.

5.6 Renovação de Chaves

Sem Estipulação.

5.7 Recuperação em Caso de Desastre ou Comprometimento

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

5.7.1 Procedimentos em Caso de Incidente ou Desastre

As cópias de segurança das chaves privadas das EC`s (geradas e mantidas de acordo com a secção 6.2.4) e dos registos arquivados (secção 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

5.7.2 Recursos Computacionais, Software e/ou Dados Corrompidos

No caso dos recursos informáticos, software e/ou dados estarem corrompidos ou existir suspeita de corrupção, podem ser obtidas as cópias de segurança das chaves privadas das EC`s e os registos arquivados, 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 Multicert suspenderá os serviços das EC`s afetadas e notificará a Entidade Supervisora.

5.7.3 Procedimentos em caso de Comprometimento de Chave Privada da Entidade

No caso da chave privada de uma das EC`s da PKI Multicert ser comprometida ou haver suspeita do seu comprometimento, são tomadas medidas apropriadas de resposta ao incidente. As respostas a esse tipo de incidente incluem:

- Notificação da Entidade Supervisora e dos Titulares de certificados emitidos no “ramo” da hierarquia de confiança da EC afetada;
- Revogação dos certificados emitidos no “ramo” da respetiva hierarquia de confiança e do certificado da EC afetada;
- Geração de novo par de chaves para a EC afetada;
- Renovação de todos os certificados emitidos no “ramo” da hierarquia de confiança da EC afetada.

5.7.4 Capacidades de Continuidade de Negócio em caso de Desastre

A Multicert dispõe dos recursos de computação, software, cópias de segurança e registos arquivados nas suas instalações secundárias de segurança, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) após um desastre natural ou outro.

5.8 Cessação da EC ou ER

Em caso de cessação de atividade como prestador de serviços de confiança, a Multicert atempadamente, com uma antecedência mínima de três meses, procede às seguintes ações:

a) Informa a Entidade Supervisora;

b) Informa os Subscritores/Titulares de certificados;

c) Revoga todos os certificados emitidos;

d) Efetua uma notificação final aos Subscritores/Titulares 2 dias antes da cessação formal da atividade;

e) Destrui ou previne a utilização, de forma definitiva, das chaves privadas;

f) Garante a transferência para retenção de toda a informação relacionada com as atividades das EC`s, nomeadamente a chave da EC, certificados, disponibilidade de CRL`s, documentação armazenada (internamente ou externamente), repositórios e armazenamento de registos de eventos dentro do período definido na secção 5.5.2.

Em caso de alterações do organismo/estrutura responsável pela gestão da atividade das EC`s, a Multicert informa de tal facto às entidades listadas nas alíneas anteriores.

6 Controlos de Segurança Técnica

Esta seção define as medidas de segurança implementadas para a PKI Multicert de forma a proteger as chaves criptográficas geradas por esta, 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 Geração e Instalação do Par de Chaves

A geração dos pares de chaves das EC`s da PKI Multicert são processados de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1 Geração do Par de Chaves

A geração de chaves criptográficas das EC`s da PKI Multicert é feita pelos Grupos de Trabalho, compostos por elementos autorizados para tal, numa cerimónia planeada e auditada de acordo com os procedimentos escritos das operações a realizar. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos envolvidos no Grupos de Trabalho.

O hardware criptográfico, usado para a geração de chaves das EC`s da PKI 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. As cópias de segurança de chaves criptográficas são efetuadas apenas usando hardware, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perda de dados, possa haver uma recuperação total e segura das chaves.

As chaves privadas para os certificados Qualificados de Assinatura Digital e Selo Eletrónico (quando não são geradas pelo Subscritor/Titular em módulo seguro) são geradas pela EC Multicert, usando hardware criptográfico que cumpre os requisitos FIPS 140-1 nível 3 e/ou Common Criteria EAL4+.

6.1.2 Entrega da Chave Privada ao Subscritor/Titular

A entrega da chave privada associada aos certificados Qualificados de Assinatura Digital e Selo Eletrónico é efetuada em dispositivo criptográfico QSCD.

No caso dos restantes tipos de certificados, quando não é requerido que a chave privada esteja em QSCD, a chave privada é fornecida pelo Subscritor.

6.1.3 Entrega da Chave Pública ao Emissor do Certificado

A chave pública é entregue à EC Multicert, de acordo com os procedimentos indicados na secção 4.1.

6.1.4 Entrega da Chave Pública da EC às *Relying Parties*

As chaves públicas das EC`s da PKI Multicert são disponibilizadas através dos respetivos certificados, conforme secção 2.2.

6.1.5 Tamanhos de Chave

Os pares de chaves devem ter 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:

- 4096 *bits* RSA para chaves das EC´s da PKI Multicert;
- 2048 *bits* RSA para as chaves associadas aos restantes certificados emitidos pelas EC`s da PKI Multicert com algoritmo de assinatura sha256RSA.

No caso das chaves RSA, o tamanho do módulo em bits é igualmente divisível por 8.

6.1.6 Geração dos Parâmetros de Chave Pública e Verificação de Qualidade

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

As chaves das EC`s 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#11.

6.1.7 Finalidades de Utilização da Chave (de acordo com o campo *key usage* X.509 v3)

De acordo com a secção 1.4 e o documento Lista de Perfis de Certificados disponível em https://pki.multicert.com.

6.2 Proteção de Chave Privada e Controlos de Engenharia de Módulo Criptográfico

Nesta secção são considerados os requisitos para proteção das chaves privadas e para os módulos criptográficos da PKI Multicert. A Multicert implementou uma combinação de controlos físicos, lógicos e procedimentais, devidamente documentados, de forma a assegurar a confidencialidade e integridade das chaves privadas da PKI Multicert.

6.2.1 Controlos e *Standards* de Módulo Criptográfico

Para a geração dos pares de chaves das EC`s da PKI Multicert, assim como para o armazenamento das chaves privadas, a Multicert utiliza um módulo criptográfico em hardware, avaliado de acordo com FIPS 140-2 Nível 3 OU de acordo com a Common Criteria (de acordo com o Perfil de Proteção EN 419 211-5).

6.2.2 Controlo Multi-Pessoal (n de m) da Chave Privada

O controlo multi-pessoal apenas é utilizado para as chaves de EC, pois a chave privada dos certificados está sob exclusivo controlo do seu titular.

A Multicert implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros de Grupos de Trabalho para efetuar operações criptográficas sensíveis na EC.

Os dados de ativação necessários para a utilização das chaves privadas das EC`s da PKI Multicert são divididos em várias partes (guardadas nas chaves PED – pequenos tokens de identificação digital, com o formato de caneta USB, identificando diferentes papéis no acesso ao HSM), acessíveis e à responsabilidade de diferentes membros dos Grupos de Trabalho. É necessário um determinado número destas partes (n) do total do número de partes (m) para ativar as chaves privadas das EC`s da PKI Multicert guardadas no módulo criptográfico em hardware.

São necessárias duas partes (n) para a ativação das chaves privadas das EC`s da PKI Multicert.

6.2.3 Custódia de Chave Privada

As chaves privadas das EC`s da PKI Multicert são armazenadas em token de hardware seguro, sendo feita uma cópia de segurança usando uma conexão direta de hardware para hardware entre os dois tokens seguros. A geração da cópia de segurança é o último passo quando é emitido um novo par de chaves para uma EC gerida pela Multicert.

O processo de cópia de segurança utiliza um HSM com duplo factor de autenticação (consola de autenticação portátil e chaves PED – pequenos tokens de identificação digitais, com a forma de caneta USB – que identificam diferentes papéis quando é feito o acesso ao HSM), em que diferentes pessoas, cada uma detendo uma chave PED, se autenticam antes que seja possível efetuar a cópia de segurança.

O token de hardware seguro com a cópia de segurança da chave privada da EC gerida pela Multicert é colocado num cofre localizado em instalações secundárias seguras e acessíveis apenas aos membros dos Grupos de Trabalho autorizados. O controlo de acesso físico a essas instalações previne o acesso não autorizado às chaves privadas.

A cópia de segurança da chave privada da EC gerida pela Multicert pode ser recuperada em caso de mau funcionamento da chave original. O processo de recuperação de chave utiliza os mesmos mecanismos de duplo factor de autenticação e com diferentes elementos, da mesma forma que é feito o processo de criação da cópia de segurança.

6.2.4 Cópia de Segurança da Chave Privada

As chaves privadas das EC`s da PKI Multicert têm pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original, conforme a secção 4.12.

6.2.5 Arquivo de Chave Privada

As chaves privadas das EC`s da PKI Multicert, sujeitas as cópias de segurança, são arquivadas conforme identificado na secção 4.12.

6.2.6 Transferência da Chave Privada para/de um Módulo Criptográfico

As chaves privadas das EC`s da PKI Multicert não são exportáveis a partir do token criptográfico FIPS 140-2 nível 3.

Mesmo que seja feita uma cópia de segurança das chaves privadas das EC`s da PKI Multicert para um outro token criptográfico, a cópia é feita diretamente, hardware para hardware, de forma a garantir o transporte das chaves entre módulos numa transmissão cifrada.

6.2.7 Armazenamento da Chave Privada em Módulo Criptográfico

As chaves privadas das EC`s da PKI Multicert são armazenadas de forma cifrada em módulos de hardware criptográfico.

6.2.8 Método de Ativação da Chave Privada

As chaves privadas das EC`s da PKI Multicert são ativadas quando o respetivo sistema é ligado. Esta ativação é efetivada através da autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de duplo factor de autenticação (consola de autenticação portátil e chaves PED – pequenos tokens de identificação digital, com o formato de caneta USB – que identificam diferentes papéis no acesso ao HSM), em que várias pessoas (membros dos Grupos de Trabalho), cada uma delas possuindo uma chave PED, são obrigadas a autenticar-se antes que seja possível efetuar a cópia de segurança.

Para a ativação das chaves privadas das EC`s da PKI Multicert é necessário, no mínimo, a intervenção de quatro elementos dos Grupos de Trabalho. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.9 Método de Desativação da Chave Privada

As chaves privadas das EC`s da PKI Multicert são desativadas quando o respetivo sistema é desligado.

Para desativar as chaves privadas é necessária, no mínimo, a intervenção de quatro elementos dos Grupos de Trabalho. Uma vez desativadas, estas permanecerão inativas até que o processo de ativação seja executado.

6.2.10 Método de Destruição da Chave Privada

As chaves privadas das EC`s da PKI Multicert (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado, assim que terminada a sua data de validade (ou se revogadas antes deste período).

A 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 das EC`s.

6.2.11 Avaliação/Nível do Módulo Criptográfico

Descrito na secção 6.2.1.

6.3 Outros Aspetos da Gestão do Par de Chaves

6.3.1 Arquivo da Chave Pública

É efetuada uma cópia de segurança de todas as chaves públicas das EC`s da PKI Multicert pelos membros dos Grupos de Trabalho, permanecendo armazenadas após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante o seu prazo de validade.

6.3.2 Períodos Operacionais do Certificado e Períodos de Utilização do Par de Chaves

O período de utilização das chaves pode ser o mesmo que o período de validade do certificado.

Os certificados assinados por uma EC específica têm que expirar antes do período de validade do par de chaves da EC.

Neste sentido a validade dos diversos tipos de certificados é a seguinte:

Tipo de Certificado	Utilização de Chave Privada	Validade Máxima do Certificado
EC Raiz da Multicert	12 anos	25 anos
EC`s Subordinadas	Sem Estipulação	12 anos e 6 meses
Validação *on-line* OCSP	4 meses	1 ano
Timestamping	1 ano	6 anos
Assinatura Digital Qualificada	Sem Estipulação	4 anos e 6 meses
Selo Eletrónico Qualificado	Sem Estipulação	3 anos
Selo Eletrónico PSD2	Sem Estipulação	2 anos
Autenticação	Sem Estipulação	4 anos e 6 meses
Assinatura Digital Avançada	Sem Estipulação	3 anos
Certificado Qualificado de Autenticação de Website PSD2	Sem Estipulação	2 anos

6.4 Dados de Ativação

6.4.1 Geração e Instalação de Dados de Ativação

Os dados de ativação necessários para a utilização das chaves privadas das EC`s da PKI Multicert são divididos em várias partes (guardadas em chaves PED – pequenos tokens de identificação digital, com o formato de caneta USB – que identificam diferentes papéis no acesso ao HSM), ficando à responsabilidade de diferentes membros dos Grupos de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves, e obedecem aos requisitos definidos pelo *standard* FIPS 140-2 nível 3

6.4.2 Proteção de Dados de Ativação

Os dados de ativação (em partes separadas e/ou palavra-passe) são memorizados e/ou armazenados em tokens que evidenciem tentativas de violação e/ou guardados em envelopes que são armazenados em cofres seguros.

As chaves privadas das EC`s da PKI Multicert são guardadas, de forma cifrada, em token criptográfico.

6.4.3 Outros Aspetos dos Dados de Ativação

Se for necessário transmitir os dados de ativação das chaves privadas, esta transmissão será protegida contra perdas de informação, roubo, alteração de dados e divulgação não autorizada.

Os dados de ativação são destruídos (por formatação e/ou destruição física) quando a chave privada associada é destruída.

6.5 Controlos de Segurança Computacional

6.5.1 Requisitos Técnicos Específicos de Segurança Computacional

O acesso aos servidores da PKI Multicert é restrito aos membros dos Grupos de Trabalho com um motivo válido para esse acesso.

A EC Multicert Root é uma EC offline, sendo apenas ativada em âmbito de manutenção periódica e desativada logo de seguida.

As EC`s Subordinadas da PKI Multicert têm um funcionamento on-line, sendo o pedido de emissão de certificados efetuado a partir do Sistema de Gestão do Ciclo de Vida dos Certificados (SGCVC) e/ou da consola de operação.

As EC`s Subordinadas da PKI Multicert e o SGCVC dispõem de dispositivos de proteção de fronteira, nomeadamente sistema firewall, e estão em conformidade com os requisitos necessários para identificação, autenticação (utilizando duplo factor de autenticação), controlo de acessos, administração, auditoria, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.5.2 Avaliação/Nível de Segurança Computacional

Os vários sistemas e produtos utilizados pela PKI Multicert são fiáveis e protegidos contra modificações.

O módulo criptográfico em Hardware das EC`s da PKI Multicert está em conformidade com o *standard* EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-2 nível 3.

6.6 Controlos Técnicos do Ciclo de Vida

6.6.1 Controlos de Desenvolvimento de Sistema

As aplicações são desenvolvidas e implementadas de acordo com as regras de desenvolvimento de sistemas e de gestão de mudanças.

É fornecida metodologia auditável que permite verificar que o software das EC`s da PKI Multicert não foi alterado antes da sua primeira utilização. Todas as configurações e alterações do software são executadas e auditadas por membros dos Grupos de Trabalho.

6.6.2 Controlos de Gestão da Segurança

A Multicert tem mecanismos e/ou Grupos de Trabalho para controlar e monitorizar a configuração dos sistemas da PKI. Quando utilizado pela primeira vez, o sistema das EC`s da PKI Multicert é verificado para garantir que o software utilizado é fidedigno, legal e que não foi alterado depois da sua instalação.

6.6.3 Controlos de Segurança do Ciclo de Vida

As operações de atualização e manutenção dos produtos e sistemas da PKI Multicert, seguem o mesmo controlo que o equipamento original e são instalados pelos membros dos Grupos de Trabalho com formação adequada para o efeito, seguindo os procedimentos definidos.

6.7 Controlos de Segurança da Rede

A PKI Multicert dispõe de dispositivos de proteção de fronteira, nomeadamente sistema firewall, e cumpre com os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditoria, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.8 Validação Cronológica

Os certificados, CRL`s e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. Todas estas entradas são assinadas digitalmente por um certificado emitido para o efeito.

7 Perfis de Certificado, CRL e OCSP

7.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo Titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através da utilização de certificados digitais X.509 v3, que são a estrutura de dados que faz a ligação entre a chave pública e o seu Subscritor. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo Subscritor.

Um certificado tem um período de validade limitado, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer software que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.

Cada certificado tem incluído um número de série único (no contexto do DN do Emissor), que é não sequencial, maior que zero (0) e contém no mínimo 64 *bits* de *output* do CSPRNG.

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar de um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC, e zero ou mais certificados adicionais de EC`s assinados por outras EC`s.

O perfil dos certificados emitidos pelas EC`s da PKI Multicert estão em conformidade com:

- Recomendação ITU.T X. 509[6];
- RFC 5280[4];
- Legislação aplicável, nacional e europeia;
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

Os perfis de certificados podem ser consultados no documento Lista de Perfis de Certificados disponível em https://pki.multicert.com.

7.1.1 Número(s) de Versão

Todos os certificados emitidos pela PKI Multicert estão em conformidade com a versão 3 do X.509.

[6] cf. ITU-T *Recommendation* X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework*.

7.1.2 Extensões do Certificado

As extensões dos certificados emitidos pela PKI Multicert estão em conformidade com o RFC 5280.

7.1.3 Identificadores de Objeto de Algoritmo

Os certificados emitidos pela PKI Multicert são assinados usando o algoritmo sha256WithRSAEncrypton (1.2.840.113549.1.1.11):

{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

7.1.4 Formatos de Nome

De acordo com o definido na secção 3.1.

7.1.5 Restrições de Nome

A Multicert pode incluir restrições de nome no campo nameConstraints, quando aplicável.

7.1.6 Identificador de Objeto de Política de Certificado

Todos os certificados emitidos pela PKI Multicert contêm os seguintes qualificadores:

"*policyQualiflierID*: 1.3.6.1.5.5.7.2.1" e "*cPSuri*", que aponta para o URI onde se encontra a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*". São incluídos outros identificadores de objetos de política de certificado, dependendo do tipo de certificado, de acordo com a secção 1.2 deste documento, e de acordo com o descrito na Lista de Perfis de Certificados (MULTICERT_PJ.ECRAIZ_428_pt) disponível em https://www.pki.multicert.com.

7.1.7 Utilização de Extensão de Restrições de Política

Sem Estipulação.

7.1.8 Sintaxe e Semânticas de Qualificadores de Política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores de certificados e autores da política de certificado. O tipo de qualificador é o "*CPSuri*", que contém um apontador, na forma de URI, para a Declaração de Práticas de Certificação publicada pela EC; e o "*userNotice explicitText*", que contém um apontador, na forma de URI, para a Política de Certificado.

7.1.9 Processamento de Semânticas para a Extensão de Políticas de Certificado Críticas

Sem Estipulação.

7.2 Perfil CRL

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, existem várias circunstâncias que podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o Titular e os dados do certificado (por exemplo, um trabalhador que termina o emprego), o comprometimento ou suspeita de comprometimento da correspondente chave privada. Nestas circunstâncias, quando a EC tem conhecimento revoga o certificado.

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC ou CRL). A CRL é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na CRL pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a CRL mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova CRL periodicamente.

O perfil de CRL`s emitidas pelas EC`s da PKI Multicert estão em conformidade com:

- ITU.T Recommendation X.509[6];
- RFC 5280[4]; e
- Legislação aplicável, nacional e europeia.

7.2.1 Número(s) de Versão

As CRL`s emitidas pela PKI Multicert estão em conformidade com a versão 2 do RFC 5280, e incluem os seguintes campos:

Campo	Valor
Version	2
Signature Algorithm	sha-256WithRSAEncryption
Issuer Name	DN da EC emissora da CRL
This Update	Data de emissão da CRL
Next Update	Data da próxima emissão de CRL
Revoked Certificates List	Lista de certificados revogados Em cada entrada da lista é incluído o número de série e data de revogação
Signature	Assinatura produzida pela EC emissora da CRL

7.2.2 CRL e Extensões da CRL

As CRL`s emitidas pela PKI Multicert têm as seguintes extensões:

Extensão	Valor
Authority Key Identifier	Identificador da EC emissora da CRL

CRL Number	Número sequencial da CRL
CRL Reason Code	Razão da revogação (opcional)

7.3 Perfil OCSP

O perfil dos certificados OCSP emitidos pela PKI Multicert estão em conformidade com:

- ITU.T recommendation X.509[6];
- RFC 6960[7]; e
- Legislação aplicável, nacional e europeia.

7.3.1 Número(s) de Versão

Os pedidos e respostas OCSP emitidos pela PKI Multicert estão em conformidade com a versão 1 do RFC 6960.

7.3.2 Extensões OCSP

Sem Estipulação.

[7] cf. RFC 69602013,X.509 Internet Public Key Infrastructure Online Certificate Status Protocol -OCSP.

8 Auditoria de Conformidade e Outras Avaliações

São realizadas auditorias internas a esta DPC e a outras regras, procedimentos, cerimónias e processos.

A PKI Multicert é sujeita a auditorias externas, realizadas por uma Entidade de Avaliação de Conformidade (CAB), de forma a avaliar a conformidade da PKI Multicert e ER`s relativamente à legislação Nacional e Europeia aplicável.

8.1 Frequência ou Circunstâncias da Avaliação

As auditorias de conformidade são realizadas anualmente. A Multicert necessita provar, através dos relatórios de auditoria (produzidos por uma Entidade de Avaliação de Conformidade), que está em conformidade com a legislação Nacional e Europeia aplicável.

8.2 Identificação/Qualificações do Avaliador

As auditorias externas de conformidade são realizadas por uma Entidade de Avaliação de Conformidade (CAB) devidamente acreditada[8].

O Organismo Nacional de Acreditação (NAB) é responsável pela credenciação das Entidades de Avaliação da Conformidade (CAB) com base da EN ISO/IEC 17065 conforme perfil da ETSI EN 319 403, estando estes capacitados a efetuar as avaliações de conformidade, resultando dessas avaliações um Relatório de Conformidade (CAR) a ser disponibilizado à Entidade Supervisora e outras partes interessadas, para avaliar a continuidade da disponibilização de serviços de confiança.

8.3 Relação do Avaliador com a Entidade Avaliada

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 ser garantida inexistência de qualquer vínculo contratual, financeiro, dependência legal ou organizacional, ou qualquer outra dependência que possa gerar conflito de interesses.

8.4 Tópicos Abrangidos pela Avaliação

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação Nacional e Europeia aplicável e com esta DPC e outras regras, procedimentos e processos (especialmente os relacionados com operações de gestão de chaves, recursos, controlos de gestão e operação, e gestão do ciclo de vida dos certificados).

[8] https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

8.5 Ações Tomadas como Resultado de Deficiências

Se de uma auditoria resultarem não conformidades, o auditor procede da seguinte forma:

a) Documenta todas as não conformidades encontradas durante a auditoria no Relatório de Avaliação de Conformidade (CAR). Dependendo da severidade das não conformidades:

   a. Falha se as não conformidades forem severas, neste caso o serviço de confiança auditado não é certificado em conformidade;

   b. Passa se as não conformidades não forem severas, neste caso o serviço de confiança auditado tem 3 meses para corrigir as não conformidades, desempenhando os passos abaixo.

b) Tendo em conta as não conformidades constantes no CAR, a entidade submetida à auditoria envia um Plano de Ações Corretivas, no qual devem estar descritas as ações, metodologia e tempo necessário para corrigir as não conformidades;

c) O CAB, depois de analisar este plano de ações toma uma das seguintes opções:

   a. Aceita as ações propostas, neste caso após as ações estarem implementadas é realizada uma auditoria de verificação para validar a eficácia da implementação das ações;

   b. Não aceita as ações propostas, neste caso o auditado tem que propor outro plano de ações.

8.6 Comunicação de Resultados

Os resultados são comunicados à Entidade Supervisora e outras partes interessadas.

9 Outras Matérias Legais e de Negócio

9.1 Taxas

9.1.1 Taxas de Emissão ou Renovação de Certificado

As taxas cobradas pela Multicert estão identificadas na sua loja online ou numa proposta formal realizada pela Multicert.

9.1.2 Taxas de Acesso a Certificado

Sem Estipulação.

9.1.3 Taxas de Acesso a Informação de Estado ou Revogação

O acesso a informação sobre o estado de certificado ou revogação (CRL e Delta CRL) é gratuita e livre.

9.1.4 Taxas para Outros Serviços

As taxas para a validação cronológica e OCSP *on-line* são identificadas numa proposta formal realizada pela Multicert.

9.1.5 Política de Reembolso

Sem Estipulação.

9.2 Responsabilidade Financeira

9.2.1 Cobertura de Seguro

A Multicert dispõe do seguro obrigatório de responsabilidade civil, conforme o artigo 20.º do Decreto-Lei n.º 12/2021, e Portaria n.º 62/2021.

9.2.2 Outros Recursos

Sem Estipulação.

9.2.3 Cobertura de Seguro ou Garantia para Utilizadores Finais

A Multicert dispõe do seguro obrigatório de responsabilidade civil, conforme o artigo 20.º do Decreto-Lei n.º 12/2021, e Portaria n.º 62/2021.

9.3 Confidencialidade de Informação de Negócio

9.3.1 Âmbito de Informação Confidencial

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

- As chaves privadas das EC`s da PKI Multicert;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
- Toda a informação de carácter pessoal fornecida à PKI Multicert durante o processo de registo dos Subscritores de certificados, salvo se houver autorização explícita para a sua divulgação e/ou se a mesma não for incluída no conteúdo do certificado emitido;
- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Informação de todos os documentos relacionados com a PKI Multicert (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 Multicert com a condição de não serem usados ou divulgados para além do âmbito dos seus deveres nos termos estabelecidos, sem autorização prévia e explícita da Multicert;
- Todas as palavras-chave, PIN`s e outros elementos de segurança relacionados com as EC`s da PKI Multicert;
- A identificação dos membros dos Grupos de Trabalho da PKI Multicert;
- A localização dos ambientes da PKI Multicert e seu conteúdo.

9.3.2 Informação fora do Âmbito de Informação Confidencial

É considera informação de acesso público:

- Política de Certificado;
- Declaração de Práticas de Certificação;
- CRL;
- Delta CRL;
- Toda a informação classificada como “Público” (a informação que não esteja expressamente considerada “pública” deve ser considerada confidencial).

A EC Multicert permite o acesso a informação não confidencial sem prejuízo dos controlos de segurança necessários para proteger a autenticidade e integridade da informação.

9.3.3 Responsabilidade de Proteção de Informação Confidencial

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 de Informação Pessoal

9.4.1 Plano de Privacidade

O Sistema de Gestão do Ciclo de Vida do Certificado (SGCVC) é responsável por implementar medidas que assegurem a privacidade de dados pessoais, de acordo com a legislação Portuguesa e Europeia aplicável.

9.4.2 Informação Tratada como Privada

É considerada informação privada toda a informação fornecida pelo Subscritor/Titular do certificado que não seja disponibilizada no certificado digital do Subscritor/Titular ou CRL.

9.4.3 Informação Não Considerada Privada

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo Subscritor/Titular do certificado que seja disponibilizada no certificado digital do Subscritor/Titular ou CRL.

9.4.4 Responsabilidade pela Proteção de Informação Privada

De acordo com a legislação Portuguesa e Europeia aplicável.

9.4.5 Notificação e Consentimento para Utilização de Informação Privada

De acordo com a legislação Portuguesa e Europeia aplicável.

9.4.6 Divulgação Resultante de Processo Judicial ou Administrativo

Sem Estipulação.

9.4.7 Outras Circunstâncias de Divulgação de Informação

Sem Estipulação.

9.5 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados, CRL e Delta CRL emitidos, OID, DPC e PC, bem como qualquer outro documento relativo à PKI Multicert, pertencem à Multicert S.A..

As chaves privadas e as chaves públicas são propriedade do Subscritor/Titular, independentemente do meio físico que se utilize para o seu armazenamento.

O Subscritor/Titular reserva sempre o direito sobre as marcas, produtos ou nome comercial contido no certificado.

9.6 Representações e Garantias

9.6.1 Representações e Garantias da EC

A Multicert S.A., como entidade prestadora de serviços de certificação, é obrigada a:

a) Desempenhar as suas operações de acordo com esta declaração de práticas;

b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado;

c) Proteger as suas chaves privadas;

d) Emitir certificados de acordo com o *standard* X.509;

e) Emitir certificados que estejam conformes com a informação conhecida no momento da sua emissão e livres de erros de entrada de dados;

f) Garantir a confidencialidade no processo de geração dos dados de criação da assinatura e na sua entrega ao Subscritor/Titular através de um procedimento seguro;

g) Utilizar sistemas e produtos confiáveis que estejam protegidos contra todas as modificações e que garantam a segurança técnica e criptográfica dos processos de certificação;

h) Utilizar sistemas confiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir a modificação de dados por pessoas não autorizadas;

i) Arquivar os certificados emitidos sem quaisquer alterações;

j) Garantir que podem determinar com precisão a data e hora em que um certificado foi emitido, revogado ou suspenso;

k) Empregar pessoal com as qualificações, conhecimento e experiência necessária para a prestação de serviços de certificação;

l) Revogar os certificados nos termos da secção 4.9 deste documento, e publicar os certificados revogados no repositório da CRL das EC`s da PKI Multicert, com a frequência estabelecida na secção 4.9.7;

m) Publicar no seu repositório a DPC e Política de Certificado aplicável garantindo o acesso às versões atuais;

n) Disponibilizar as versões anteriores da DPC;

o) Notificar com a rapidez necessária, por email, os Subscritores/Titulares de certificado caso uma das EC`s revogue ou suspenda o certificado, indicando a razão correspondente para tal ação;

p) Colaborar com as auditorias realizadas pela Entidade de Avaliação de Conformidade;

q) Operar de acordo com a legislação aplicável;

r) Proteger eventuais chaves existentes que estejam sob a sua custódia;

s) Garantir a disponibilidade da CRL de acordo com o disposto na secção 2;

t) Comunicar com uma antecedência mínima de 2 meses a todos os Titulares dos certificados emitidos assim como à Entidade Supervisora, em caso de cessar a sua atividade;

u) Cumprir com as especificações contidas no regulamento Europeu sobre Proteção de Dados Pessoais;

v) Manter toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento, durante 7 anos após a expiração do certificado;

w) Disponibilizar os certificados das EC`s da PKI Multicert.

9.6.2 Representações e Garantias da ER

As Entidades de Registo são obrigadas a:

a) Desempenhar as suas operações de acordo com esta declaração de práticas;

b) Permitir a emissão de certificados livres de erros de entrada de dados;

c) Garantir a confidencialidade no processo de geração dos dados de criação da assinatura e na sua entrega ao Subscritor/Titular através de um procedimento seguro;

d) Utilizar sistemas e produtos confiáveis que estejam protegidos contra todas as modificações e que garantam a segurança técnica e criptográfica dos processos de certificação;

e) Arquivar os certificados emitidos sem quaisquer alterações;

f) Empregar pessoal com as qualificações, conhecimento e experiência necessária para a prestação de serviços de confiança;

g) Colaborar com as auditorias realizadas pela Entidade de Avaliação de Conformidade;

h) Operar de acordo com a legislação aplicável, nomeadamente de acordo com o Regulamento 910/2014;

i) Proteger eventuais chaves existentes que estejam sob a sua custódia;

j) Comunicar com uma antecedência mínima de dois meses a todos os Titulares dos certificados emitidos assim como à Entidade Supervisora, em caso de cessar a sua atividade;

k) Cumprir com as especificações contidas no regulamento Europeu sobre Proteção de Dados Pessoais;

l) Manter toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento, durante 7 anos após a expiração do certificado.

9.6.3 Representações e Garantias do Subscritor/Titular

É obrigação do Subscritor/Titular do certificado emitido:

a) Limitar e ajustar a utilização do certificado de acordo com as finalidades previstas na Política de Certificado, Condições Gerais de Emissão de Certificado Digital, e secção da 1.4 da DPC;

b) Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;

c) Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita do comprometimento da chave privada correspondente à chave pública contida no certificado, ou outra razão constante na secção 4.9;

d) Não utilizar o certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspenso ou expirado o seu período de validade;

e) Submeter à Entidade de Certificação (ou Entidade de Registo) a informação que considere exata e completa em relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;

f) 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 S.A..

9.6.4 Representações e Garantias da *Relying Party*

É obrigação das partes que confiem nos certificados emitidos pelas EC`s da PKI Multicert:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na correspondente Política de Certificado e secção 1.4 da DPC;

b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;

c) Assumir a responsabilidade pela correta verificação das assinaturas digitais;

d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados nos quais confia;

e) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia, e aceitar sujeitar-se às mesmas;

f) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como razão para a revogação do mesmo, utilizando os meios que a Multicert S.A. indique na sua DPC.

9.6.5 Representações e Garantias de outros Participantes

Sem Estipulação.

9.7 Renúncia de Garantias

A Multicert S.A. recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

9.8 Limitações de Responsabilidade

A Multicert S.A., enquanto Entidade de Certificação:

a) Responde pelos atos e omissões no exercício da sua atividade de acordo com o Artigo 15º do Decreto-lei 12/2021;

b) Responde pelos prejuízos que cause aos Subscritores/Titulares ou a terceiros pela falta ou atraso na inclusão de um certificado revogado ou suspenso no serviço de consulta de validade dos certificados, uma vez que tenha conhecimento dele;

c) Assume toda a responsabilidade mediante terceiros pelas funções necessárias à prestação de serviços de confiança, no âmbito da atuação dos Subscritores/Titulares;

d) A sua responsabilidade de administração / gestão assenta numa base objetiva e abrange todo o risco que os particulares sofram sempre que este seja consequência do funcionamento normal ou anormal dos seus serviços;

e) Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando os limites da utilização possível não tenham sido consignados no certificado, de forma clara reconhecida por terceiros;

f) Não responde quando o Subscritor/Titular supera os limites que constam no certificado quanto às suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao Subscritor/Titular;

g) Não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que constam no certificado quanto às suas possíveis utilizações;

h) Não assume qualquer responsabilidade no caso de perda ou prejuízo:

   i. Dos serviços prestados, em caso de guerra, desastre natural ou qualquer outro motivo de força maior;

   ii. Resultante da utilização dos certificados quando esta utilização exceda os limites estabelecidos na DPC e PC;

   iii. Resultante do uso indevido ou fraudulento dos certificados ou CRL`s emitidas pelas EC`s da PKI Multicert.

9.9 Indemnizações

De acordo com a legislação em vigor.

9.10 Prazo e Terminação

9.10.1 Prazo

Os documentos relacionados com a PKI Multicert (incluindo esta DPC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Trabalho de Gestão.

Esta DPC entra em vigor desde o momento de sua publicação no repositório da Multicert.

Esta DPC mantém-se em vigor enquanto não for revogada expressamente pela emissão de uma nova versão.

9.10.2 Terminação

As alterações são adequadamente registadas com indicação de uma versão menor.

As alterações tornam-se efetivas após a aprovação do Grupo de Trabalho de Gestão e a publicação no repositório de uma versão maior.

9.10.3 Efeito da Terminação e Sobrevivência

As obrigações e restrições estabelecidas nesta DPC, relativamente a auditorias, informação confidencial, arquivo de registos, obrigações e responsabilidades, criadas sob a sua vigência, subsistirão após a sua substituição por uma nova versão em tudo o que não se oponha a esta.

9.11 Notificações Individuais e Comunicações aos Participantes

Qualquer notificação relacionada com a DPC deve ser feita por correio eletrónico assinado digitalmente, formulários assinados enviados por correio, ou outros, dependendo da criticidade e assunto da comunicação. Estas notificações devem ser enviadas para os contactos indicados na secção 1.5.

9.12 Alterações

9.12.1 Procedimento para Alteração

As alterações a esta DPC são realizadas pelo Grupo de Trabalho de Autenticação. Podem ser submetidas ao Grupo de Trabalho de Autenticação sugestões de alterações para serem analisadas, através dos contactos fornecidos na secção 1.5.

O Grupo de Trabalho de Autenticação regista as alterações da revisão em versões menores na DPC. Quando se encontra pronta para aprovação uma nova versão da DPC, o Grupo de Trabalho de Autenticação submete o documento para aprovação do Grupo de Trabalho de Gestão, sendo incrementada uma versão maior à DPC.

9.12.2 Mecanismo e Período de Notificação

As alterações à DPC são registadas na tabela Histórico de Versões, contendo identificação da versão, data, e detalhes das alterações feitas.

Quando é aprovada uma nova versão maior da DPC pelo Grupo de Trabalho de Gestão, é publicada no repositório da Multicert uma versão atualizada deste documento.

9.12.3 Circunstâncias nas quais o OID deve ser Alterado

Se o Grupo de Trabalho de Autenticação determinar que é necessário alterar o OID correspondente à DPC ou PC, propõe essa alteração ao Grupo de Trabalho de Gestão. Neste caso, é criado um novo documento DPC ou PC com um OID diferente.

De outra forma, as alterações não devem requerer a alteração do OID da DPC ou PC.

9.13 Disposições de Resolução de Conflito

Em caso de litígio o consumidor pode recorrer a uma Entidade de Resolução Alternativa de Litígios de consumo. A Lista oficial de tais Entidades está disponível no Portal do Consumidor em www.consumidor.pt.

Sem prejuízo da possibilidade de recurso prévio à mediação, caso não seja obtido acordo entre as partes no âmbito de tal procedimento quanto a qualquer conflito decorrente da interpretação, aplicação ou execução do presente formulário de emissão, qualquer uma das partes poderá recorrer à via judicial, ficando desde já fixado como foro competente para o efeito a Comarca de Lisboa.

9.14 Legislação Aplicável

A Multicert, enquanto entidade que presta serviços de confiança, tais como os serviços de certificação digital, é obrigada a cumprir os requisitos estabelecidos na atual legislação portuguesa e europeia.

9.15 Conformidade com a Legislação Aplicável

Ver secção 9.14.

9.16 Outras Disposições

9.16.1 Acordo Completo

Todas as *relying parties* assumem na totalidade o conteúdo da última versão desta DPC.

9.16.2 Atribuição

As partes que operam sob esta DPC ou acordos aplicáveis não podem atribuir os seus direitos ou obrigações sem o prévio consentimento por escrito da Multicert.

9.16.3 Divisibilidade

Se uma disposição desta DPC, incluindo cláusulas de limitação de responsabilidade, for considerada ineficaz ou não executável, o restante desta DPC deve ser interpretado no sentido da intenção original das partes.

Qualquer disposição desta DPC que estabeleça uma limitação de responsabilidade deve ser separável e independente de qualquer outra disposição e deve ser aplicada como tal.

9.16.4 Execução (Honorários de Advogados e Renúncia de Direitos)

A Multicert pode requerer a indemnização e honorários advocatórios de uma parte por danos, perdas e despesas relacionadas à conduta dessa parte. A falha da Multicert em aplicar uma cláusula desta DPC não renuncia ao direito da Multicert de aplicar a mesma cláusula posteriormente ou ao direito de aplicar quaisquer outras cláusulas desta DPC. Para ter efeito, qualquer renúncia deve ser feita por escrito e assinada pela Multicert.

9.16.5 Força Maior

As cláusulas de força maior estão incluídas nas Condições Gerais de Emissão de Certificado Digital.

9.17 Outras Provisões

Sem Estipulação.

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: 2023.09.20 08:38:49 +01'00'