multicert
Engineering for digital security

Declaração de Práticas de Certificação da Entidade de Certificação Raiz da MULTICERT

Política

MULTICERT_PJ.ECRAIZ_24.1.1_0001_pt.doc

Identificação do Projeto: ECRaiz da MULTICERT

Identificação da CA: MULTICERT Root CA

Nível de Acesso: Público

Versão: 3.0

Data: 07/10/2015

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

Identificador do documento: MULTICERT_PJ.ECRAIZ_24.1.1_0001_pt.doc

Palavras-chave: DPC

Tipologia documental: Política

Título: Declaração de Práticas de Certificação da Entidade de Certificação Raiz da MULTICERT

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 07/10/2015

Versão atual: 3.0

Identificação do Projeto: ECRaiz da MULTICERT

Identificação da CA: MULTICERT Root CA

Cliente: ---

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	21/03/2014	Versão Aprovada	MULTICERT S.A.
1.1	26/06/2014	Alteração de Morada	MULTICERT S.A.
2.0	10/07/2014	Versão aprovada	MULTICERT S.A.
2.1	28/07/2015	Revisão	MULTICERT S.A.
3.0	01/10/2015	Verão aprovada	MULTICERT S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRaiz_24.1.2_0001_pt.pdf	Política de Certificado da MULTICERT Root CA	MULTICERT S.A.
MULTICERT_PJ.ECRaiz_24.1.13_0001_pt.pdf	Declaração de Divulgação de Princípios	MULTICERT S.A.

Sumário

1 Introdução

Objetivos do Documento

O objetivo deste documento é definir os procedimentos e práticas levadas a cabo pela MULTICERT no desenrolar da sua atividade de certificação digital, no âmbito da EC Raiz da MULTICERT. Este documento é referido como sendo a Declaração de Práticas de Certificação (DPC) da EC Raiz da MULTICERT.

Público-Alvo

Este documento deve estar disponível publicamente e é destinado a todas as entidades que se relacionem, de alguma forma, com a EC Raiz da MULTICERT.

Estrutura do Documento

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF, no documento RFC 3647[1], de acordo também com a estrutura recomendada pelo ETSI TS 102 042[2].

Os primeiros dez capítulos são dedicados a descrever os procedimentos e práticas mais importantes no âmbito da certificação digital da Entidade de Certificação Raiz da MULTICERT. O capítulo 11 descreve as matérias legais.

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

[2] *cf. ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*, v2.4.1

2 Contexto Geral

O presente documento é uma Declaração de Práticas de Certificação, doravante designada de DPC, cujo objetivo se prende com a definição de um conjunto de práticas para a emissão e validação de Certificados e para a garantia de fiabilidade. Não se pretende nomear regras legais ou obrigações, mas antes informar, pretendendo-se assim 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 seguidas pela Entidade de Certificação Raiz da MULTICERT (MULTICERT Root CA) e, explica o que um Certificado fornece, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada, para confiarem nos Certificados emitidos pela MULTICERT Root CA. Este documento pode sofrer atualizações regulares.

2.1 Visão Geral

As práticas de criação, assinatura e emissão de Certificados, assim como de revogação de certificados inválidos, levadas a cabo por uma Entidade de Certificação (EC) são fundamentais para garantir a fiabilidade e confiança de uma Infraestrutura de Chaves Públicas (ou PKI – *Public Key Infrastructure*).

Esta DPC aplica-se especificamente à MULTICERT Root CA sendo que respeita e implementa as seguintes normas:

- RFC 3647: *Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, 2003;
- RFC 5280: *Internet X.509 PKI - Certificate and CRL Profile*, 2008;
- *ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates,* v2.4.1 e*;*
- *CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.0.*

2.2 Designação e Identificação do Documento

Este documento é a Declaração de Práticas de Certificação da MULTICERT Root CA. A DPC é representada num certificado, através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento o 1.3.6.1.4.1.25070.1.1.1.0.7 e o OID associado à Política de Certificados é o 1.3.6.1.4.1.25070.1.1.1.0.2.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.1.0.7
Data de Emissão	Setembro 2015
Validade	1 Ano
Localização	https://pki.multicert.com/index.html

2.3 Participantes na Infraestrutura de Chave Pública

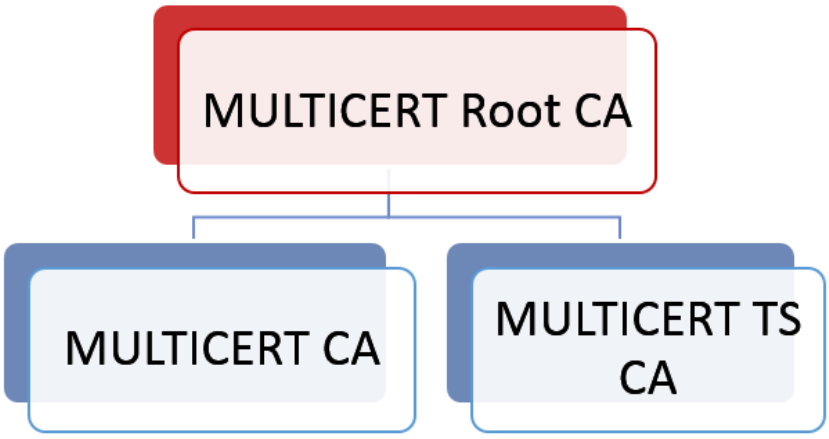
2.3.1 Entidade Certificadoras

A MULTICERT, enquanto Entidade Gestora da PKI da MULTICERT, cumpre as disposições previstas nas normas e legislação aplicável, assumindo as competências aí descritas sendo responsável por fornecer serviços e assegurar os procedimentos (mesmo recorrendo à subcontratação de terceiras partes) que possam garantir as funcionalidades a seguir indicadas:

1. Geração dos pares de chaves criptográficas associadas a cada uma da Entidades Certificadoras;
2. Receção e validação dos pedidos de emissão de certificados realizados pelas Entidades de Certificação (EC`s) subordinadas bem como os demais subscritores;
3. Emissão de certificados, relativos a pedidos de certificados que estejam de acordo com o formato requerido pelas Entidade de Certificação da MULTICERT;
4. Receção e validação dos pedidos de suspensão, reativação e revogação de certificados;
5. Publicação dos certificados (quando, onde e se apropriado) e de informação acerca do seu estado;
6. Assegurar a contínua disponibilidade da informação pública, para todos os seus utilizadores;

A MULTICERT atualmente detém três Entidades de Certificação:

- MULTICERT Root Certification Authority (MULTICERT Root CA);
- MULTICERT Certification Authority (MULTICERT CA);
- MULTICERT Trust Services Certification Authority (MULTICERT TS CA).



2.3.1.1 MULTICERT Root Certification Authority (MULTICERT Root CA)

A MULTICERT Root CA é uma entidade certificadora credenciada pela Autoridade Nacional de Segurança, de acordo com o ETSI 102 042, estando deste modo habilitada, legalmente, a emitir certificados para Entidades de Certificação Subordinadas.

MULTICERT Root CA está incluída em vários programas de reconhecimento de Entidades Certificadoras de topo de *browsers* e sistemas, promovendo assim a sua disseminação global.

CERTIFICATE INFORMATION	
Nome Distinto	`CN=MULTICERT Root Certification Authority, O=MULTICERT, Serviços de Certificação Electrónica S.A., C=PT`
Algoritmo de Assinatura	`sha256RSA`
Nº de Série	`6e e9 1e f8 b2 d5 c9 ac`
Validade	`13/03/2014 a 13/07/2039`
Marca Digital	`c5 81 41 59 a9 64 74 73 e8 71 07 2a e5 32 8d 2d 9d 90 d6 9e`

2.3.1.2 MULTICERT Certification Authority (MULTICERT CA)

A MULTICERT CA é uma entidade certificadora credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada, legalmente, a emitir todo o tipo de certificados digitais, incluindo os certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação). Insere-se em duas hierarquias de confiança:

- Hierarquia de confiança auto-assinada própria, para efeitos de independência em relação a outras hierarquias de confiança;
- Hierarquia de confiança internacional, com credenciação WebTrust (http://www.webtrust.org/) e com presença na maioria dos sistemas operativos e navegadores Web.

Deste modo, a MULTICERT CA é reconhecida na maioria dos sistemas operativos e *browsers*, sendo a sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores.

A MULTICERT CA emite certificados de,

- Assinatura Qualificada para pessoa singular;
- Assinatura Qualificada de Qualidade;
- Assinatura Qualificada para representação de pessoa coletiva;
- Autenticação para pessoa singular e coletiva;
- Assinatura Avançada para pessoa singular e coletiva;
- Certificados SSL para servidor web;
- Certificados de Aplicação;
- Serviços da PKI MULTICERT, i.e., certificados para serviços necessários no âmbito da PKI MULTICERT:
    - Validação on-line OCSP.

INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	CN=MULTICERT Entidade de Certificação 001, OU = Entidade de Certificação Credenciada, O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT
Algoritmo de Assinatura	Sha1RSA
Nº de Série	07 27 8e f0
Validade	29/05/2020
Marca Digital	ef 2e 98 f4 42 ee cd 10 b9 8f 2a da 72 16 09 8c e4 83 53 18

INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	CN=MULTICERT Certificate Authority 002, OU=Accredited Certification Authority, O=MULTICERT – Serviços de Certificação Electrónica S.A., C=PT
Algoritmo de Assinatura	SHA256RSA
Nº de Série	17 33 10 19 7f 6e 01 c1
Validade	13/03/2014 a 12/07/2025
Marca Digital	02 a7 f8 8d c1 76 71 e7 a6 93 82 b3 26 4e f2 1e 5d b9 3b 4e

2.3.1.3 MULTICERT Trust Services Certification Authority (MULTICERT TS CA)

A MULTICERT TS CA é uma entidade certificadora credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/gns), conforme previsto na legislação portuguesa e europeia. Insere-se em duas hierarquias de confiança:

- Hierarquia de confiança auto-assinada própria, para efeitos de independência em relação a outras hierarquias de confiança;
- Hierarquia de confiança internacional, com credenciação WebTrust (http://www.webtrust.org/) e com presença na maioria dos sistemas operativos e navegadores Web.

Deste modo, a MULTICERT TS CA é reconhecida na maioria dos sistemas operativos e navegadores Web, sendo a sua principal função providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores.

A MULTICERT TS CA emite certificados de:

- *Code Signing*;
- *Object Signing*;
- Serviços da PKI MULTICERT, i.e., certificados para serviços necessários no âmbito da PKI MULTICERT:
  - *Timestamping*;
  - TSL (Trust Service Status List).

INFORMAÇÃO DO 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
Algoritmo de Assinatura	SHA256RSA
Nº de Série	64 f5 57 61 cc 29 0e 51
Validade	14/03/2014 to 13/07/2025
Marca Digital	59 9e 95 f8 93 e0 67 91 2e 87 65 bf 4c dd f1 e8 1e 94 96 40

2.3.2 A Entidade de Registo

A Entidade de Registo (ER) é uma entidade autorizada a reunir e verificar informação de identidade de EC`s subordinadas e a informação exigida pela MULTICERT para cada tipo de certificado a emitir. A MULTICERT poderá agir como ER e/ou estabelecer acordos com outras entidades para que estas desempenhem esse papel.

2.3.3 Outros participantes

2.3.3.1 Autoridade Credenciadora

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

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

A Autoridade Credenciadora é uma das "peças" que contribui para a confiabilidade dos Certificados Qualificados, pelas competências que exerce sobre as EC que os emitem. No âmbito das suas funções, a Autoridade Credenciadora, 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 tão diversificados como a segurança física, o *hardware* e *software*, os procedimentos de acesso e de operação;

b) **Fiscalização**: procedimento assente em inspeções efetuadas às Entidades de Certificação, com vista a regularmente verificar parâmetros de conformidade;

c) **Auditor de Segurança**, figura independente do círculo de influência da EC e que lhe é exigida.

2.3.3.2 Auditor de Segurança

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

2.4 Utilização do Certificado

Os certificados emitidos no domínio da PKI da MULTICERT são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança:

a) Controlo de acessos;
b) Confidencialidade;
c) Integridade;
d) Autenticação e,
e) Não-repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a PKI da MULTICERT proporciona. Assim, os serviços de identificação e autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves.

2.4.1 Utilização adequada

Os requisitos e regras definidos neste documento, aplicam-se a todos os certificados emitidos pela MULTICERT Root CA.

Os certificados emitidos para equipamentos tecnológicos, têm como objetivo a sua utilização em serviços de autenticação e no estabelecimento de canais cifrados.

Os certificados emitidos para efeitos de utilização por serviços de confidencialidade, emitidos com base nas regras aqui definidas, podem ser utilizados para processar informação classificada até ao grau de CONFIDENCIAL, quando utilizados sobre redes públicas (p.e. Internet). Na sua utilização em redes proprietárias, o grau de classificação da informação deverá ser definido pelo organismo nacional com responsabilidades no âmbito do tratamento da informação/matéria classificada.

Os certificados emitidos na PKI da MULTICERT são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido na hierarquia da PKI da MULTICERT, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado emitido sob a PKI da MULTICERT.

2.4.2 Utilização não autorizada

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

Os certificados emitidos na PKI da MULTICERT não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela PKI da MLTICERT, 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.

2.5 Gestão das Políticas

2.5.1 Entidade responsável pela gestão do documento

A gestão desta declaração de práticas de certificação é da responsabilidade do Grupo de Trabalho de Autenticação da PKI da MULTICERT.

2.5.2 Contato

NOME	Grupo de Trabalho de Autenticação da EC MULTICERT
Morada:	MULTICERT S.A. Lagoas Park, Edifício 3, Piso 3 2740-266 Porto Salvo Oeiras
Correio eletrónico:	pki.documentacao@multicert.com
Página Internet:	www.multicert.com
Telefone:	+351 217 123 010
Fax:	+351 217 123 011

2.5.3 Entidade responsável pela determinação da conformidade da DPC relativamente à Política

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

2.5.4 Procedimentos para Aprovação da DPC

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

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

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

3 Responsabilidades de Publicação e Armazenamento

A MULTICERT reserva o direito de publicar informação relativa a certificados digitais emitidos por esta, num repositório disponível *online*, assim como de publicar informação sobre o estado do certificado em repositórios de terceiras partes.

A MULTICERT mantém um repositório de documentos *online* onde divulga informação sobre as suas práticas, procedimentos e conteúdo de determinadas políticas, incluindo a DPC.

Todas as partes associadas à emissão, utilização ou gestão de certificados da MULTICERT são aqui notificadas de que a MULTICERT pode publicar informação submetida, no seu repositório acessível publicamente, no sentido de disponibilizar informação sobre o estado do certificado digital.

A MULTICERT abstém-se de disponibilizar publicamente determinados elementos de documentos relacionados com controlos de segurança, procedimentos, políticas de segurança internas, etc. No entanto, estes elementos são sujeitos a auditorias formais de acreditação, como a ETSI TS 102 042.

3.1 Repositórios

A MULTICERT S.A. é responsável pelas funções de repositório da EC Raiz da MULTICERT, publicando entre outras, informação relativa às práticas adotadas e o estado dos certificados emitidos (LRC).

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

- Mínimo de 99,990% de respostas a pedidos de obtenção da LRC;
- Mínimo de 99,990% de respostas a pedidos do documento da DPC;
- Número máximo de pedidos de LRC: 50 pedidos/minuto;
- Número máximo de pedidos da DPC: 50 pedidos/minuto;
- Número médio de pedidos de LRC: 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:

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

3.2 Publicação de informação de certificação

A MULTICERT S.A. mantém um repositório em ambiente *web*, permitindo que as Partes Confiantes efetuem pesquisas *online*, relativas à revogação e outra informação referente ao estado dos Certificados.

A MULTICERT S.A. disponibiliza sempre a seguinte informação pública *online*:

- Cópia eletrónica desta DPC e Políticas de Certificados (PC) mais atuais da MULTICERT Root CA, assinada eletronicamente, por indivíduo devidamente autorizado e com certificado digital atribuído para o efeito:
- DPC da MULTICERT Root CA disponibilizada no URI: **https://pki.multicert.com/index.html**;
- PC do certificado auto-assinado da MULTICERT Root CA disponibilizada no URI: **https://pki.multicert.com/index.html**;
- LRC da MULTICERT Root CA – URI: **https://pki.multicert.com/index.html**
- Certificado da MULTICERT Root CA – URI: **https://pki.multicert.com/index.html**;
- Outra informação relevante – URI: **https://pki.multicert.com/index.html**.

Adicionalmente, serão conservadas, fora do repositório público de acesso livre, todas as versões anteriores da PC e DPC da MULTICERT Root CA. No entanto, poderão ser disponibilizadas a quem as solicite, desde que justificada a sua necessidade.

3.3 Periodicidade de publicação

As atualizações a esta DPC e respetivas PC, darão origem à sua publicação imediatamente após a sua aprovação pelo Grupo de Gestão, de acordo com a secção 10.2.

O certificado da MULTICERT Root CA é publicado imediatamente após a emissão. A LRC será publicada, no mínimo, a cada 4 meses.

3.4 Controlo de acesso aos repositórios

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

4 Identificação e Autenticação

4.1 Atribuição de Nomes

Esta secção descreve os procedimentos usados para autenticar as entidades certificadas antes de lhe serem emitidos certificados, bem como questões relativas a disputas de nomes.

4.1.1 Tipos de Nomes

A MULTICERT garante a emissão de certificados contendo um *Distinguished Name* (DN) **X.500**. Emite certificados para os requerentes que submetem documentação contendo um nome verificável.

A MULTICERT assegurará, dentro da sua infraestrutura de confiança, a não existência de certificados que, contendo o mesmo DN, possam identificar entidades distintas.

4.1.2 Necessidade de Nomes Significativos

A MULTICERT assegurará que os nomes usados nos certificados por ela emitidos, identificam de uma forma significativa os seus utilizadores. Isto é, será assegurado que o DN usado é apropriado para o utilizador em questão e que o componente *common name* do DN representa o utilizador de uma forma facilmente compreensível pelas pessoas. Contudo, poderá a MULTICERT emitir certificados sob pseudónimo, desde que os mesmos sejam dessa forma identificados.

4.1.3 Interpretação de Formatos de Nome

As regras para interpretação de nomes estão definidas em documento próprio, de acesso restrito a pessoas autorizadas pela MULTICERT.

4.1.4 Unicidade dos Nomes

A MULTICERT controlará os nomes existentes, de forma a garantir que um certificado contém um DN único, relativo a apenas uma entidade e que não é ambíguo.

4.1.5 Resolução de Disputas de Nomes

A MULTICERT será responsável por atribuir e aprovar os DN`s. Será também responsável por resolver quaisquer disputas que possam surgir.

4.1.6 Reconhecimento, Autenticação e Papéis das Marcas Registadas

Os nomes emitidos pela MULTICERT respeitarão o máximo possível as marcas registadas. A MULTICERT não permitirá deliberadamente a utilização de nomes registados cuja entidade não possa

provar serem de sua propriedade. Contudo a MULTICERT poderá recusar a emissão de certificados com nomes de marcas registadas se entender que outra identificação é mais conveniente.

4.1.7 Método de Prova da Posse da Chave Privada

Nos casos em que a MULTICERT não seja a responsável pela geração do par de chaves criptográficas, a atribuir ao utilizador, a MULTICERT assegurará que o utilizador possui a chave privada correspondente à chave pública constante no pedido de certificado antes de proceder à sua emissão.

O método de prova será necessariamente tão mais complexo e preciso consoante a importância do tipo de certificado pedido, encontrando-se documentado na Política e Certificado do certificado em causa.

4.2 Validação de Identidade Entidade no Registo Inicial

A MULTICERT é responsável por autenticar a identidade dos clientes candidatos à obtenção de um certificado. As formas de proceder a essa autenticação incluem:

- Assegurar que o cliente existe e autorizou a emissão do certificado;
- Garantir que o cliente está ciente que para ser integrado na hierarquia da MULTICERT Root CA tem que cumprir com o estabelecido neste documento, tal como indicado na alínea 4.2.1;

Assegurar que os representantes legais da MULTICERT Root CA aceitaram o cliente em questão dentro da sua hierarquia.O processo de registo e autenticação será assegurado pelo seguinte: é da responsabilidade da ER registar corretamente os utilizadores finais do certificado, usando todos os meios necessários para os identificar positivamente e de forma legal. Entre as operações a realizar para atingir este objetivo contam-se:

1. Verificar em documentos oficialmente reconhecidos pelo Estado em que o subscritor (individual ou organização) está registado:
    a. O nome completo;
    b. Os dados de contato, incluindo o endereço de contato;
    c. A sua identificação única legal.
2. Garantir a presença física do subscritor no momento da realização do registo, a não ser que já exista uma relação de confiança previamente baseada nessa presença física do subscritor;

Os procedimentos para identificação e autenticação de subscritores previamente desconhecidos deverão seguir as seguintes regras:

1. O subscritor ou o seu representante legal (no caso de uma pessoa coletiva) deverão apresentar-se fisicamente à MULTICERT;
2. A identificação física deverá ser autenticada contra provas identificativas que devem estar de acordo com as provisões seguintes:
    a. Ser oficialmente reconhecidas na jurisdição em que o subscritor está registado;
    b. Indicar o nome completo do subscritor e o seu endereço oficial;
    c. Ter pelo menos uma prova de identidade que contenha uma fotografia do subscritor (sempre aplicável);
    d. Indicar um número de registo único dentro da jurisdição em que tiver sido emitido;
3. No caso de certificados para subscritores não humanos, os processos de autenticação referidos serão aplicados às pessoas que estejam autorizadas a pedir certificados para os subscritores especificados.

3. A MULTICERT verificará que cada candidato à obtenção de um certificado tem o direito de obter esse certificado e, caso a obtenção do certificado implique também a obtenção de atributos ou privilégios de qualquer espécie, o candidato realmente tem direito a esses privilégios e atributos;

4. Quando necessário, a MULTICERT exigirá que a entidade requerente de um certificado prepare e submeta um Pedido lógico de Certificado apropriado à EC;

5. Também quando necessário, a MULTICERT verificará a correção da informação incluída no Pedido lógico de Certificado da entidade requerente.

4.2.1 Acordo com o Subscritor

A MULTICERT guardará registo do acordo assinado com o subscritor, incluindo:

1. Acordo dos termos e condições com o subscritor. Caso o subscritor do certificado seja distinto do sujeito, este último também será informado sobre os termos e condições;
2. Consentimento para a manutenção de registos por parte da MULTICERT, com a informação usada no registo, bem como informação de subsequentes acontecimentos relativos ao acordo e ao seu objeto;
3. Permissão para passar esta informação a terceiros sob certas condições;
4. Permissão para passar informação sobre o estado dos certificados emitidos, ao abrigo do acordo, a terceiros não descriminados.

4.2.1.1 Pedido de Certificado

A MULTICERT:

1. Exigirá que uma entidade requerente de um certificado prepare e submeta os dados apropriados ao pedido, como especificado nesta DPC;
2. Quando necessário, exigirá que a entidade final requisitante submeta a sua chave pública para certificação, numa mensagem assinada digitalmente usando a chave privada a que corresponde a chave pública constante no pedido, de forma a:
    a. Permitir a deteção de erros no processo de certificação;
    b. Provar a posse da chave privada relativa à chave pública a certificar.
3. Utiliza a chave pública contida no Pedido lógico de Certificado da entidade requisitante para verificar a assinatura da entidade requisitante no Pedido lógico de Certificado submetido;
4. Verifica a autenticidade da submissão, da ER, de acordo com esta DPC;
5. Verificará a assinatura da ER no Pedido lógico de Certificado;
6. Verifica o Pedido lógico de Certificado para verificar se este contém erros ou omissões de acordo com esta DPC;
7. Verifica a unicidade do DN da entidade requisitante dentro da sua infraestrutura;
8. Aceita o Pedido lógico de Certificado vindo da entidade requisitante, cuja identidade foi validade;
9. Quando detetar chaves públicas repetidas o Pedido lógico de Certificado é rejeitado.

4.2.2 Autenticação Presencial de Entidades Individuais

A autenticação presencial do representante autorizado das organizações candidatas a um certificado será baseada em, pelo menos, duas formas de identificação emitidas pelo governo (em que pelo menos uma terá de ser um documento com fotografia, tal como, um passaporte). A capacidade da pessoa agir

em nome da organização candidata será também autenticada, através da apresentação de documentação em papel, indicando este facto.

A informação descrita acima tem de ser validada pela MULTICERT aquando da devolução dos formulários de inscrição completamente preenchidos. A MULTICERT será responsável por verificar a identidade dos representantes pessoalmente.

4.3 Identificação e Autenticação para pedidos de renovação de chaves

4.3.1 Identificação e autenticação para renovação de chaves, de rotina

Muitas implementações da PKI permitem a emissão, automática ou facilitada, de certificados de atualização, para um subscritor, antes do fim do período de validade do certificado existente. Esta ação é conhecida como renovação de rotina, e é possível devido ao facto de já existir uma relação de confiança com o subscritor.

No entanto, dependendo do certificado em questão, é necessário garantir que as condições originais necessárias para obter o certificado em questão se mantêm, isto é:

1. O indivíduo/organização ainda existe e autorizou a emissão do certificado;
2. O indivíduo/organização continua a obedecer aos requisitos de associação;
3. O indivíduo/organização possui a chave privada correspondente à nova chave pública expedida para certificação;
4. A MULTICERT aceita a continuidade do indivíduo/organização dentro da sua hierarquia.

A renovação só poderá ser repetida um máximo de 3 vezes sem que seja necessário repetir um novo registo do utilizador. Porém, a Política de Certificado do certificado a renovar pode especificar expressamente outras condições de renovação, inclusive contrárias a esta.

4.3.2 Renovação após Revogação

Se um certificado é revogado, o indivíduo/organização será sujeito a todo o processo inicial de registo, de forma a obter um novo certificado. Porém, a Política de Certificado do certificado a renovar pode especificar expressamente outras condições de renovação, inclusive contrárias a esta.

4.4 Pedido de Revogação

O pedido de revogação deve obedecer às condições descritas em pormenor na secção 5.7.

5 Requisitos Operacionais do Ciclo de Vida do Certificado

5.1 Pedido de Certificados

O pedido de certificado deve iniciado telefonicamente através do número 217123010.

5.2 Emissão dos Certificados

5.2.1 Procedimento para a emissão de certificado

A emissão do certificado é efetuada por meio de uma cerimónia que decorre na zona de alta segurança da PKI da MULTICERT e, em que se encontram presentes:

- Os representantes legais da entidade subordinada requerente ou o(s) representante(s) nomeado(s) para esta cerimónia;
- 4 membros dos Grupos de Trabalho já que a segregação de funções não possibilita a presença de um número inferior de elementos;
- Um Auditor Qualificado – para testemunhar a geração do par de chaves da MULTICERT Root CA e emitir um relatório a relatar o cumprimento dos requisitos do processo de geração de chaves por parte da MULTICERT Root CA e a utilização de controlos para garantir a integridade e confidencialidade do par de chaves;
- Quaisquer observadores, aceites simultaneamente pelos membros do Grupo de Trabalho e pelos representantes da entidade subordinada requerente.

A cerimónia de emissão de certificado é constituída pelos seguintes passos:

- Identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que o(s) representante(s) da entidade subordinada requerente e os membros dos Grupo de Trabalho têm os poderes necessários para os atos a praticar;
- Representante(s) da entidade subordinada requerente entregam, em mão, o CD/DVD e o formulário de emissão do certificado aos membros do Grupo de Trabalho da MULTICERT Root CA. O formulário é datado e assinado pelos membros do Grupo de Trabalho que o devolvem ao(s) representantes da entidade subordinada requerente;
- Os membros do Grupo de Trabalho efetuam o procedimento de arranque de processamento da MULTICERT Root CA e emitem o certificado (correspondente ao PKCS#10 fornecido no CD/DVD) em formato PEM;
- Os membros do Grupo de Trabalho arquivam o certificado em formato PEM num CD/DVD e preenchem o formulário de receção e aceitação de certificado em duplicado;
- Após a assinatura de ambas as cópias do formulário de receção e aceitação de certificado pelo(s) representante(s) da entidade subordinada e pelos membros do Grupo de Trabalho, os membros do Grupo de Trabalho entregam o CD/DVD com o certificado em formato PEM ao(s) representante(s) da entidade subordinada;

- A cerimónia de emissão fica terminada com a execução do procedimento de finalização de processamento da MULTICERT Root CA, pelos membros do Grupo de Trabalho.

O certificado emitido inicia a sua vigência no momento da sua emissão.

5.2.2 Notificação da emissão do certificado ao titular

A emissão do certificado é efetuada de forma presencial, de acordo com a secção anterior.

5.3 Aceitação do Certificado

5.3.1 Procedimento para a aceitação de certificado

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) da entidade subordinada, de acordo com a cerimónia de emissão (conforme secção 5.2.1).

Note-se que antes de ser disponibilizado o certificado aos representantes, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que:

a) É tomado conhecimento dos direitos e responsabilidades;

b) É tomado conhecimento das funcionalidades e conteúdo do certificado;

c) É aceite formalmente o certificado e as suas condições de utilização assinando para o efeito o Formulário de Receção de certificado.

5.3.2 Publicação do certificado

A MULTICERT Root CA não publica os certificados emitidos, disponibilizando-o integralmente aos representantes, com os constrangimentos definidos no ponto 5.3.1.

5.3.3 Notificação da emissão de certificado a outras entidades

Nada a assinalar.

5.3.4 Uso do certificado e da chave privada pelo titular

Os titulares de certificados (representantes) utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "*keyUsage*") e sempre com propósitos legais.

A sua utilização apenas é permitida:

a) A quem estiver designado no campo "*Subject*" do certificado;

b) De acordo com as condições definidas na secção 2.4;

c) Enquanto o certificado se mantiver válido e não estiver na LRC da MULTICERT Root CA.

Adicionalmente:

- O certificado de EC subordinada só pode ser utilizado para assinar certificados e respetiva LRC, assim como certificados necessários para a operação e serviços da EC subordinados;
- O certificado de Validação *on-line* OCSP tem como objetivo a sua utilização em servidores OCSP;

5.3.5 Uso do certificado e da chave pública pelas partes confiantes

Na utilização do certificado e da chave pública, as partes confiantes apenas podem confiar nos certificados, tendo em conta apenas o que é estabelecido nesta DPC e na respetiva Política de Certificação. Para isso devem, entre outras, garantir o cumprimento das seguintes condições:

a) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;

b) Ser responsável pela sua correta utilização;

c) Ler e entender os termos e condições descritos nas Politicas e práticas de certificação;

d) Verificar os certificados (validação de cadeias de confiança) e LRC, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

5.4 Renovação de Certificados

A renovação de um certificado é o processo em que a emissão de um novo certificado utiliza os dados anteriores do certificado, não havendo alteração das chaves ou qualquer outra informação, com exceção do período de validade do certificado.

Esta prática não é suportada pela PKI da MULTICERT.

5.4.1 Motivos para renovação de certificado

Nada a assinalar.

5.4.2 Quem pode submeter o pedido de renovação de certificado

Nada a assinalar.

5.4.3 Processamento do pedido de renovação de certificado

Nada a assinalar.

5.4.4 Notificação de emissão de novo certificado ao titular

Nada a assinalar.

5.4.5 Procedimentos para aceitação de certificado

Nada a assinalar.

5.4.6 Publicação de certificado após renovação

Nada a assinalar.

5.4.7 Notificação da emissão do certificado a outras entidades

Nada a assinalar.

5.5 Renovação de certificado com geração de novo par de chaves

A renovação de chaves do certificado (*certificate re-key*) é o processo em que um titular gera um novo par de chaves e submete o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito da PKI da MULTICERT, é designado por renovação de certificado com geração de novo par de chaves.

A renovação de certificado com geração de novo par de chaves é feita de acordo com o estabelecido na secção 5.2.

5.5.1 Motivo para a renovação de certificado com geração de novo par de chaves

É motivo válido para a renovação de certificado com geração de novo par de chaves, sempre e quando se verifique que:

a) O certificado está a expirar;

b) O par de chaves está a atingir o período de utilização previsto;

c) A informação que deu origem ao certificado sofre alterações.

5.5.2 Quem pode submeter o pedido de certificação de uma nova chave pública

Tal como na secção 5.1.

5.5.3 Processamento do pedido de renovação de certificado com geração de novo par de chaves

Tal como na secção 5.2.

5.5.4 Notificação da emissão de novo certificado ao titular

Tal como na secção 5.2.2.

5.5.5 Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves

Tal como na secção 5.3.1.

5.5.6 Publicação de certificado renovado com geração de novo par de chaves

Tal como na secção 5.3.2.

5.5.7 Notificação da emissão de certificado renovado a outras entidades

Tal como na secção 5.3.3.

5.6 Modificação de certificados

A alteração de certificados é o processo em que é emitido um certificado para um titular, mantendo as respetivas chaves, havendo apenas alterações na informação do certificado.

Esta prática não é suportada pela PKI da MULTICERT.

5.6.1 Motivos para alteração do certificado

Nada a assinalar.

5.6.2 Quem pode submeter o pedido de alteração de certificado

Nada a assinalar.

5.6.3 Processamento do pedido de alteração de certificado

Nada a assinalar.

5.6.4 Notificação da emissão de certificado alterado ao titular

Nada a assinalar.

5.6.5 Procedimentos para aceitação de certificado alterado

Nada a assinalar.

5.6.6 Publicação do certificado alterado

Nada a assinalar.

5.6.7 Notificação da emissão de certificado alterado a outras entidades

Nada a assinalar.

5.7 Suspensão e Revogação de Certificados

5.7.1 Circunstâncias para Suspensão

A MULTICERT Root CA não efetua suspensões.

5.7.2 Quem pode pedir a Suspensão

Nada a assinalar.

5.7.3 Procedimento para um Pedido de Suspensão

Nada a assinalar.

5.7.4 Limites do Período de Suspensão

Nada a assinalar.

5.7.5 Motivos para Revogação

Um certificado pode ser revogado por qualquer uma das seguintes razões:

1. Comprometimento ou suspeita de comprometimento da chave privada (MULTICERT Root CA ou EC subordinada);
2. Perda da chave privada;
3. Inexatidões graves nos dados fornecidos;
4. Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/*token* criptográfico);
5. Utilização do certificado para atividades abusivas;
6. Risco de comprometimento da chave (por exemplo, devido à fraqueza do algoritmo ou tamanho de chave);
7. Cessação de funções.

O certificado é revogado no prazo máximo de 7 dias.

5.7.6 Solicitar a Revogação

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 5.7.5, os seguintes:

1. Os responsáveis legais da Entidade de Certificação Subordinada;
2. A MULTICERT S.A.;
3. Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

A MULTICERT Root CA guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado de Entidade Certificadora Subordinada.

5.7.7 Procedimento para solicitação de Revogação

Os procedimentos a serem seguidos no pedido de revogação de certificado são os seguintes:

1. Todos os pedidos de revogação devem ser endereçados para a MULTICERT S.A. por escrito ou por mensagem eletrónica assinada digitalmente, em formulário próprio de pedido de revogação;
2. Identificação e autenticação da entidade que efetua o pedido de revogação;
3. Registo e arquivo do formulário de pedido de revogação;
4. Análise do pedido de revogação pelo Grupo de Trabalho de Autenticação da PKI da MULTICERT, que propõe ao Grupo de Trabalho de Gestão a aprovação ou recusa do pedido de revogação;
5. Mediante o parecer do Grupo de Trabalho de Autenticação da PKI da MULTICERT, o Grupo de trabalho de Gestão, decide a aprovação ou recusa do pedido de revogação do certificado;
6. Sempre que se decidir revogar um certificado, a revogação é publicada na respetiva LRC.

Em qualquer dos casos, é arquivada a descrição pormenorizada de todo o processo de decisão, ficando documentado:

1. Data do pedido de revogação;
2. Nome do titular do certificado;
3. Exposição pormenorizada dos motivos para o pedido de revogação;
4. Nome e funções da pessoa que solicita a revogação;
5. Informação de contacto da pessoa que solicita a revogação;
6. Assinatura da pessoa que solicita a revogação.

5.7.8 Processamento do Pedido de Revogação

O pedido de revogação deve ser tratado de forma imediata, pelo que em caso algum poderá ser superior a 7 dias.

5.7.9 Requisitos de verificação da revogação pelas partes confiantes

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das LRC ou num servidor de verificação do estado *online* (via OCSP).

5.7.10 Frequência de Emissão de LRC`s (se aplicável)

A MULTICERT Root CA publica uma nova LRC no repositório, sempre que haja uma revogação. Quando não existam alterações ao estado de validade dos certificados, ou seja, se nenhuma revogação se tiver produzido, a MULTICERT Root CA disponibiliza uma nova LRC a cada 4 meses.

O período máximo entre a emissão e publicação da LRC não deverá ultrapassar os 30 minutos.

Todas as LRC`s emitidas pela MULTICERT são assinadas digitalmente pela MULTICERT ou uma entidade designada pela MULTICERT.

A MULTICERT assegura que, em condições normais de operação, mantém recursos que permitem fornecer um tempo de resposta de 10 segundos para obtenção da LRC.

5.7.11 Requisitos para Verificação de LRC`s

A informação mais atualizada acerca do estado de revogação de um certificado estará disponível através de Servidores com serviços de verificação de estado fornecidos pela MULTICERT. Todos os interessados deverão consultar estes para saberem a informação mais recente acerca do estado de um certificado.

5.7.12 Outras Formas de Anúncio de Revogação

A MULTICERT Root CA dispõe de serviços de validação OCSP do estado dos certificados de forma *online*. Esse serviço poderá ser acedido em http://ocsp.multicert.com/ocsp/.

5.8 Mudança de Chaves

Todas as Entidade de Certificação Subordinadas reconhecidas pela MULTICERT Root CA, serão notificadas (oralmente ou por meios eletrónicos) antes da atualização do seu par de chaves. Será da inteira responsabilidade das Entidades de Certificação Subordinadas a notificação de toda a estrutura diretamente abaixo de si, até aos titulares dos certificados digitais.

6 Medidas de segurança física, de 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 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 falta de segurança pode comprometer as operações da PKI da MULTICERT.

6.1 Medidas de segurança física

6.1.1 Localização física e tipo de construção

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

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

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

a) Paredes em alvenaria, betão ou tijolo;

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

c) Inexistência de janelas;

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

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

- Perímetros de segurança claramente definidos;
- Paredes, chão e teto em alvenaria, sem janelas, que impedem acessos não autorizados;
- Trancas e fechaduras anti-roubo de alta segurança nas portas de acesso ao ambiente de segurança;

- O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;
- Acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

6.1.2 Acesso físico ao local

Os sistemas da PKI da MULTICERT estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança) de acordo com a NT D-02[3], garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

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

O acesso ao cartão de identificação vermelho obriga a um duplo controlo de autenticação de acesso individual. 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 controlo duplo, cada um deles utilizando dois fatores de autenticação, incluindo autenticação biométrica. O *hardware* criptográfico e *tokens* físicos seguros dispõem de proteção adicional, sendo guardados em cofres e armários seguros. 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.

6.1.3 Energia e ar condicionado

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

- Alimentação de energia garantindo alimentação contínua ininterrupta com a potência suficiente para manter autonomamente a rede elétrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações elétricas que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia, e geradores de eletricidade a diesel); e
- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente. Um sensor de temperatura, ativa um alerta GSM sempre que a temperatura atinge valores anormais. Este alerta GSM consiste em telefonemas com uma mensagem previamente gravada, para os elementos da equipa de manutenção.

[3] GNS/NT D-02 – Requisitos mínimos de Segurança Física de Instalações de Entidades Certificadoras

6.1.4 Exposição à água

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

6.1.5 Prevenção e proteção contra incêndio

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

- Sistemas de deteção e alarme de incêndio estão instalados nos vários níveis físicos de segurança;
- Equipamento fixo e móvel de extinção de incêndios estão disponíveis, 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;
- Procedimentos de emergência bem definidos, em caso de incêndio.

6.1.6 Salvaguarda de suportes de armazenamento

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

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

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

6.1.7 Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível deverão ser 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. Equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Outros equipamentos de armazenamento (discos rígidos, *tapes*, ...)

deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

6.1.8 Instalações externas (alternativa) para recuperação de segurança

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).

6.2 Medida de segurança dos processos

A atividade de uma Entidade Certificadora (daqui em diante denominada por EC) depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque:

- Dados os requisitos de segurança inerentes ao funcionamento de uma EC 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;
- Quando uma mesma entidade é detentora de várias EC de diferentes níveis de segurança ou hierarquia, por vezes é desejável que os recursos humanos associados a uma EC não acumulem funções (ou pelo menos as mesmas) numa EC distinta.

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

6.2.1 Grupos de Trabalho

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

A PKI da MULTICERT estabeleceu que os papéis de confiança fossem agrupados em sete categorias diferentes (que correspondem a seis Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticados, eventualmente pertencentes a diferentes Grupos de Trabalho.

6.2.1.1 Grupo de Trabalho de Auditoria

É responsável por efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a operacionalidade da EC. Este grupo deve ter um mínimo de 2 (dois) membros.

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exatidão dos processos e cerimónias da EC;
- Registar todas as operações sensíveis;

- Investigar suspeitas de fraudes procedimentais;
- Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;
- Registar todos os procedimentos passíveis de auditoria;
- Registar os resultados de todas as ações por si realizadas;
- Assumir o papel de "Auditor de Sistema"[4];
- Validar que todos os recursos utilizados são seguros.

Adicionalmente[5]:

- O auditor externo, tem de ser independente da autoridade de certificação; deve ter competência reconhecida; experiência e qualificações sólidas na área da segurança de informação no desempenho de auditorias de segurança e no uso do *standard* ISO/IEC 17799; e precisa de ser credenciado pela "Autoridade Nacional de Segurança";
- A entidade de certificação necessita de fazer prova, através de uma auditoria anual e de um relatório de segurança (produzido por um auditor de segurança acreditado) que a avaliação do risco foi analisada, e que foram identificadas e implementadas todas as medidas necessárias à segurança da informação;
- O auditor de segurança necessita garantir que nenhum dos seus membros executa funções parciais ou discriminatórias ligadas à entidade de certificação. Necessita também de garantir que nenhum dos auditores trabalhou para a entidade de certificação nos últimos 3 anos, nem que tenham qualquer tipo de acordo ou contrato legal com a entidade de certificação.

6.2.1.2 Grupo de Trabalho de Operação

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

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Produção" e do "Ambiente Operação";
- Realizar as tarefas de rotina da EC, incluindo operações de cópias de segurança dos seus sistemas,
- Execução de tarefas de monitorização dos sistemas EC;
- Monitorizar, reportar e quantificar todos os incidentes e avarias de *software* e *hardware*, despoletando os processos apropriados à correção das mesmas;
- Assumir o papel de "Administrador de Sistema" [4];
- Assumir o papel de "Operador de Sistema" [4] e,
- Assumir o papel de "Administrador de Registo" [4].

Nenhum membro deste grupo está autorizado a entrar no Ambiente de Produção sem a presença de, pelo menos, um outro elemento pertencente a outro grupo de trabalho

[4] cf. Decreto Regulamentar n.º 25/2004, de 15 de Julho. Artigo 29.
[5] cf. Decreto Regulamentar n.º 25/2004, de 15 de Julho. Artigo 30.

6.2.1.3 Grupo de Trabalho de Autenticação

É responsável por propor todas as políticas da EC, assegurando que se encontram atualizadas.

É ainda responsável por assegurar a gestão, guarda e disponibilidade (nas situações previstas) das palavras-passe (não pessoais) e dos *tokens* de autorização.

Nenhum membro deste grupo está autorizado a entrar no Ambiente de Produção sem a presença de, pelo menos, um outro elemento pertencente a outro grupo de trabalho As responsabilidades deste grupo são:

- Definir todas as políticas da EC e garantir que se encontram atualizadas e adaptadas à realidade desta;
- Assegurar que as PC's da EC são suportadas pela DPC da EC;
- Assegurar que todos os documentos relevantes e relacionados, direta ou indiretamente, com o funcionamento da EC se encontram armazenados no Ambiente de Informação;
- Gestão do "Ambiente de Autenticação";
- Gestão de todas as palavras-passe não pessoais;
- Manter um inventário atualizado de todos os *tokens* de autenticação usados no "Ambiente de Operação", e quando os *tokens* estão à responsabilidade de algum(ns) membro(s), registar a identificação desse(s) membro(s), e guardar estes registos no "Ambiente de Autenticação";
- Manter um inventário atualizado de todas as palavras-passe usadas no "Ambiente de Operação", e quando as palavras-passe estão à responsabilidade de algum(ns) membro(s), registar a identificação desse(s) membro(s), e guardar estes registos no "Ambiente de Autenticação";
- Garantir que cada membro dos restantes grupos não detém mais *tokens* de autenticação do que os estritamente necessários à execução das responsabilidades de que está incumbido;
- Garantir que cada membro dos restantes grupos não detém mais palavras-passe de autenticação do que as estritamente necessárias para a execução das responsabilidades de que está incumbido;
- Registar a devolução dos *tokens* de autenticação usados pelos membros dos restantes grupos;
- Registar trocas de palavras-passe de autenticação usadas pelos membros dos restantes grupos;
- Registar a perca de *tokens* de autenticação, descrevendo adequadamente a situação que lhe deu origem;
- Registar sempre que uma palavra-passe de autenticação é comprometida, descrevendo adequadamente a situação que o originou;
- Avaliar os riscos de negócio resultantes da perca de um *token* ou o comprometimento de uma palavra-passe de autenticação;
- Tomar medidas ativas de modo a não comprometer cada Ambiente de Produção derivado da perca de um *token*, ou do comprometimento de alguma palavra-passe de autenticação e,
- Avaliar pedidos de replicação de documentação.
- Assumir o papel de *Administrador de Segurança*, conforme definido no artigo 29º do Decreto Regulamentar n.º 25/2004

6.2.1.4 Grupo de Trabalho de Monitorização e Controlo

A missão deste grupo consiste na 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.

Tendo em conta este enquadramento, o Grupo de Trabalho de Monitorização e Controlo interage com o Grupo de Trabalho de Auditoria para efeitos de contribuições para o esforço de melhoria contínua dos compromissos de segurança da PKI da MULTICERT, assumindo ainda um papel relevante no controlo de incidentes e respetivo processo de gestão.

As responsabilidades deste grupo são:

- Instalar e configurar o *software* de base da PKI da MULTICERT;
- Instalar, interligar e configurar o *hardware* da PKI da MULTICERT;
- Configurar palavras-passe iniciais que irão ser alteradas posteriormente pelo Grupo de Trabalho de Autenticação e,
- Preparar comunicados sobre:
    - As palavras-passe iniciais;
    - *Hash* do(s) CD(s) de instalação utilizados;
- A lista de todos os artefactos (univocamente identificados) indispensáveis à inicialização e, operação da PKI. Consolidar e analisar a monitorização dos recursos utilizados na PKI da MULTICERT;
- Garantir a melhoria contínua do "Processo de gestão de Incidentes" e a respetiva gestão operacional;
- Colaborar com o Grupo de Trabalho de Auditoria com o objetivo de promover ações de melhoria contínua;
- Monitorizar o funcionamento dos alarmes existentes;
- Fazer passagens a produção requeridas pela pré-produção;
- Monitorizar eventos, gerir alarmes e classificar incidentes;
- Definir, apoiar a implementação e a melhoria contínua de procedimentos para resposta a incidentes;
- Fazer passagens a produção requeridas pela pré-produção.

6.2.1.5 Grupo de Trabalho de Gestão

É responsável pela nomeação dos membros dos restantes grupos[6] e pela guarda de alguns artefactos sensíveis (*tokens* de autenticação, etc.). Este membro deve ter um mínimo de 4 (quatro) membros.

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Gestão";
- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Autenticação;

[6] À exceção do Grupo de Trabalho de Instalação, do Grupo de Trabalho de Auditoria e do Grupo de Trabalho de Custódia

- Designar os membros dos restantes grupos de trabalho (à exceção do Grupo de Trabalho de Instalação, do Grupo de Trabalho de Auditoria e do Grupo de Trabalho de Custódia);
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados.

6.2.1.6 Grupo de Trabalho de Custódia

É responsável pela custódia de alguns artefactos sensíveis (*tokens* de autenticação, etc.), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições[7]. Note-se que, no sentido de melhorar os níveis de segurança, operacionalidade e continuidade de negócio da EC, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de artefactos. Este grupo deve fazer uso dos vários ambientes seguros disponibilizados para a guarda deste tipo de itens.

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Custódia" respetivo;
- Custódia de artefactos sensíveis (*tokens* de autenticação, etc.) usando os meios adequados que respondam às necessidades de segurança respetivas e,
- Disponibilização segura destes itens a membros de grupos autorizados e explicitamente indicados com permissões de acesso a esses itens, após o cumprimento dos procedimentos apropriados de segurança.

6.2.2 Número de pessoas exigidas por tarefa

Existem rigorosos procedimentos de controlo que obrigam à divisão de responsabilidades baseada 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 da EC 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, controlos adicionais de acesso são utilizados 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.

6.2.3 Funções que requerem separação de responsabilidades

A matriz seguinte define as incompatibilidades (assinaladas por ✖) entre a pertença ao grupo/subgrupo identificado na coluna esquerda e a pertença ao grupo/subgrupo identificado na primeira linha, no contexto desta EC:

[7] Definidas para cada um dos artefactos à sua guarda

Se pertence ao Grupo/Subgrupo...	Pode pertencer ao Grupo?	Operação	Autenticação	Auditoria	Custódia	Gestão
Operação			✘	✘	✘	✘
Autenticação		✘		✘	✘	✘
Auditoria		✘	✘		✘	✘
Custódia		✘	✘	✘		✘
Gestão		✘	✘	✘	✘	

6.3 Medidas de Segurança de Pessoal

6.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Todo o pessoal que desempenhe funções de confiança na PKI da MULTICERT deve cumprir os seguintes requisitos:

- Ter sido nomeado formalmente para a função a desempenhar;
- Apresentar provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas inerentes à sua função;
- Ter credenciação mínima Nacional Confidencial (ou equivalente);
- Ter recebido formação e treino adequado para o desempenho da respetiva função;
- Garantir confidencialidade, relativamente a informação sensível sobre a EC ou dados de identificação dos titulares;
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função e,
- Garantir que não desempenha funções que possam causar conflito com as suas responsabilidades nas atividades da EC.

6.3.2 Procedimento 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[4] inclui:

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

6.3.3 Requisitos de formação e treino

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 adicionalmente 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 na PKI da MULTICERT;
e) Política de Certificados e Declaração de Práticas de Certificação;
f) Recuperação face a desastres;
g) Procedimentos para a continuidade da atividade e,
h) Aspetos legais básicos relativos à prestação de serviços de certificação.

6.3.4 Frequência e requisitos para ações de reciclagem

Sempre que necessário será 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 exista qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto à PKI da MULTICERT;
- Sempre que são introduzidas alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos da PKI da MULTICERT.

6.3.5 Frequência e sequência da rotação de funções

Nada a assinalar.

6.3.6 Sanções para ações não autorizadas

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

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

6.3.7 Requisitos para prestadores de serviços

Consultores ou prestadores de serviços independentes, tem permissão de acesso à zona de alta segurança desde de que estejam sempre acompanhados e diretamente supervisionados pelos membros do Grupo de Trabalho e ficando o seu acesso registado no Livro de Presenças próprio.

6.3.8 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.

6.4 Procedimentos de auditoria de segurança

6.4.1 Tipo de eventos registados

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

- Tentativas de acesso (com e sem sucesso) para solicitar, gerar, assinar, emitir ou revogar chaves de certificados;
- Tentativas de acesso (com e sem sucesso) para criar, modificar ou apagar informação dos titulares dos certificados;
- Tentativas de acesso (com e sem sucesso) e alterações dos parâmetros de segurança do sistema operativo;
- Emissão e publicação de LRC's;
- Arranque e paragem de aplicações;
- Tentativas de acesso (com e sem sucesso) de início e fim de sessão;
- Tentativas de acesso (com e sem sucesso) de criar, modificar, apagar contas do sistema;
- Cópias de segurança, recuperação ou arquivo dos dados;
- Alterações ou atualizações de *software* e *hardware*;
- Manutenção dos sistemas;
- Operações realizadas por membros dos Grupos de Trabalho;
- Alteração de Recursos Humanos;
- Tentativas de acesso (com e sem sucesso) às instalações por parte de pessoal autorizado ou não;
- A cerimónia de geração de chaves e sistemas envolvidos na mesma, tais como servidores aplicacionais, base de dados e sistema operativo.

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, quando aplicável;

- Descrição do evento.

6.4.2 Frequência da auditoria de registos

Os registos são analisados e revistos anualmente pelos elementos do grupo de trabalho de Auditoria, e adicionalmente sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. Ações tomadas, baseadas na informação dos registos são também documentadas.

6.4.3 Período de retenção dos registos de auditoria

Os registos são mantidos disponíveis durante pelo menos 2 (dois) meses após processamento, e depois arquivados nos termos descritos na secção 6.5.

6.4.4 Proteção dos registos de auditoria

Os registos são analisados exclusivamente por membros do Grupo de Trabalho de Auditoria e reportados ao Grupo de Gestão.

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.

As cópias de segurança da PKI da MULTICERT são armazenadas em local seguro e em cofres que cumprem a norma EN 1143.

A destruição de um arquivo de auditoria só poderá ser efetuada após autorização expressa do Grupo de Gestão e executada na presença de, no mínimo dois elementos, um elemento de autenticação e um de auditoria, sendo que este ato deverá ficar registado em log de Auditoria.

6.4.5 Procedimentos para a cópia de segurança dos registos

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

6.4.6 Sistema de recolha de registos (Interno / Externo)

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

6.4.7 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.

6.4.8 Avaliação de vulnerabilidades

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

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

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

6.5 Arquivo de registos

6.5.1 Tipo de dados arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 6.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

As informações e eventos que são registados e arquivados são:

a) Os registos de auditoria especificados no ponto 6.4.1 desta DPC;

b) As cópias de segurança dos sistemas que compõem a infraestrutura da PKI da MULTICERT;

c) Toda a documentação relativa ao ciclo de vida dos certificados, designadamente:

- Procedimentos de emissão e revogação de certificados de serviço;

- Formulários de emissão e receção dos certificados de serviço;

d) Acordos de confidencialidade;

e) Protocolos estabelecidos com as Entidades Subscritoras;

f) Contratos estabelecidos entre a PKI da MULTICERT e outras entidades - apenas disponibilizados a quem solicitar a sua visualização, após avaliação e aprovação prévia do pedido;

g) Autorizações de acesso aos sistemas de informação;

h) Acessos aos artefactos existentes nas custódias.

6.5.2 Período de retenção em arquivo

Os dados sujeitos a arquivo são retidos pelo período de tempo definido pela legislação nacional.

6.5.3 Proteção dos arquivos

O arquivo é protegido de modo a que:

- Apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo;
- O arquivo é protegido contra qualquer modificação ou tentativa de o remover;
- O arquivo é protegido contra a deterioração dos media onde é guardado, através de migração periódica para media novo;
- O arquivo é protegido contra a obsolescência do *hardware*, sistemas operativos e outros *software*, pela conservação do *hardware*, sistemas operativos e outros *software* que passam a

fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal;

- Os arquivos são guardados de modo seguro em ambientes externos seguros. As cópias de segurança da PKI da MULTICERT são armazenadas em locais seguros e em cofres que cumprem a norma EN 1143.

6.5.4 Procedimentos para as cópias de segurança do arquivo

Cópias de segurança dos arquivos são efetuadas de modo incremental ou total e guardados em dispositivos WORM (*Write Once Read Many*).

6.5.5 Requisitos para validação cronológica dos registos

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

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

Os sistemas de recolha de dados de arquivo são internos.

6.5.7 Procedimentos de recuperação e verificação de informação arquivada

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

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

6.6 Renovação de chaves

Apenas as entidades de certificação subordinadas da PKI da MULTICERT com certificados válidos podem requerer a renovação do respetivo par de chaves, desde que a geração de novo par de chaves esteja conforme a secção 6.7.

6.7 Recuperação em caso de desastre ou comprometimento

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

6.7.1 Procedimentos em caso de incidente ou comprometimento

As cópias de segurança das chaves privadas da MULTICERT Root CA (geradas e mantidas de acordo com a secção 7.2.3.1) e dos registos arquivados (secção 6.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre. No caso de comprometimento da chave privada da MULTICERT Root CA, esta deverá tomar as seguintes ações:

- Proceder à sua revogação imediata;
- Revogar todos os certificados dela, dependentes;
- Informar todos os titulares dos seus certificados e terceiras partes conhecidas;
- Informar todas as Entidades que compõem a PKI da MULTICERT.

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

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

Se for confirmado que os recursos informáticos, *software* e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a MULTICERT CA Root suspenderá os seus serviços e notificará todas as Entidades envolvidas. Caso se verifique que esta situação tenha afetado certificados emitidos, proceder-se-á à notificação dos titulares dos mesmos e à revogação dos respetivos certificados.

6.7.3 Procedimentos em caso de comprometimento da chave privada da entidade

No caso da chave privada da MULTICERT Root CA ser comprometida ou haver suspeita do seu comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. As respostas a esse incidente podem incluir:

- Informar a Autoridade Nacional de Segurança (ANS);
- Revogação do certificado da MULTICERT Root CA e de todos os certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT Root CA;
- Notificação das EC subordinadas, todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT Root CA;
- Geração de novo par de chaves para a MULTICERT Root CA e inclusão nos vários sistemas/*browsers*;
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT Root CA.

6.7.4 Capacidade de continuidade da atividade em caso de desastre

A PKI da 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) com base em procedimentos definidos no Plano de Contingência, após um desastre natural ou outro.

6.8 Procedimentos em caso de extinção de EC ou ER

Em caso de cessação de atividade como prestador de serviços de Certificação, a MULTICERT Root CA deve, atempadamente, com uma antecedência mínima de três meses, proceder às seguintes ações:

a) Informar a Autoridade Nacional de Segurança (ANS);

b) Informar todas as Entidades envolvidas;

c) Informar todos os titulares de certificados;

d) Revogar todos os certificados emitidos;

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

f) Destruir ou impedir a utilização, de modo definitivo, das chaves privadas;

g) Garantir a transferência e manutenção (para retenção por outra organização) de toda a informação relativa à atividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos, durante o período de tempo legalmente exigido.

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

7 MEDIDAS DE SEGURANÇA TÉCNICAS

Esta secção define as medidas de segurança implementadas pela PKI da MULTICERT para a MULTICERT Root CA, de forma a proteger 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.

7.1 Geração e instalação do par de chaves

A geração dos pares de chaves da MULTICERT Root CA é processada de acordo com os requisitos e algoritmos definidos nesta política.

7.1.1 Geração do par de chaves

A geração de chaves criptográficas da MULTICERT Root CA é feito por um Grupo de Trabalho, composto por elementos autorizados para tal, numa cerimónia planeada e auditada de acordo com procedimentos escritos das operações a realizar. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos envolvidos no Grupo de Trabalho.

O *hardware* criptográfico, usado para a geração de chaves da MULTICERT Root CA, cumpre os requisitos FIPS 140-2 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 perca de dados, possa haver uma recuperação total e segura das chaves.

A geração do par de chaves da MULTICERT Root CA é efetuada por elementos autorizados dos Grupos de trabalho num *hardware* criptográfico que cumpre os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+.

O funcionamento da MULTICERT Root CA é efetuado em modo *offline*.

7.1.2 Entrega da chave privada ao titular

A MULTICERT Root CA não gera a chave privada associada aos certificados que emite.

7.1.3 Entrega da chave pública ao emissor do certificado

A chave pública é entregue à MULTICERT Root CA, de acordo com os procedimentos indicados na secção 5.2.2.

7.1.4 Entrega da chave pública da EC às partes confiantes

A chave pública da MULTICERT Root CA será disponibilizada através do certificado da MULTICERT Root CA, conforme secção 5.3.2.

7.1.5 Dimensão das chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptanálise 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 a chave da MULTICERT Root CA.

7.1.6 Geração dos parâmetros da chave pública e verificação da qualidade

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

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

7.1.7 Fins a que se destinam as chaves (campo "*key usage*" X.509 v3)

O campo "*keyUsage*" dos certificados, utilizado de acordo com o recomendado no *RFC 5280*[8], inclui as seguintes utilizações:

a) Key Certificate Signature

b) CRL Signature

7.2 Proteção da chave privada e caraterísticas do módulo criptográfico

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

7.2.1 Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da MULTICERT Root CA assim como para o armazenamento das chaves privadas, a PKI da MULTICERT utiliza módulo criptográfico em *hardware* que cumpre as seguintes normas:

- Segurança Física
    - *Common Criteria* EAL 4+ e/ou

[8] cf. RFC 5280: *Internet X.509 PKI - Certificate and CRL Profile*

- FIPS 140-2, nível 3

– Certificações Regulamentares
  - U/L 1950 & CSA C22.2 *safety compliant*
  - FCC Part 15 – Class B
  - Certificação ISO – 9002

– Papéis
  - Autenticação de dois fatores

– Geração de números aleatórios
  - *ANSI* X9.17 (Anexo C)

7.2.2 Controlo multi-pessoal (*n* de *m*) para a 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 PKI da MULTICERT implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efetuar operações criptográficas sensíveis na EC.

Os dados de ativação necessários para a utilização da chave privada da MULTICERT Root CA são divididos em várias partes (guardadas nas chaves PED – pequenos *tokens* de identificação digital, com o formato de chaves físicas, identificadoras de diferentes papéis no acesso à HSM), acessíveis e à responsabilidade de diferentes membros do Grupo de Trabalho. Um determinado número destas partes (*n*) do total número de partes (*m*) é necessário para ativar a chave privada da MULTICERT Root CA guardada no módulo criptográfico em *hardware*. São necessárias duas (n) partes para a ativação da chave privada da MULTICERT Root CA.

7.2.3 Retenção da chave privada (*key escrow*)

A MULTICERT Root CA só efetua a retenção da sua chave privada.

7.2.3.1 Políticas e práticas de recuperação de chaves

A chave privada da MULTICERT Root CA é armazenada num *token hardware* de segurança, sendo efetuada uma cópia de segurança utilizando uma ligação direta hardware a *hardware* entre dois *tokens* de segurança. A geração da cópia de segurança é o último passo da emissão de um novo par de chaves da MULTICERT Root CA.

A cerimónia de cópia de segurança utiliza um HSM com autenticação de dois fatores (consola de autenticação portátil e chaves PED – pequenos *tokens* de identificação digital, com o formato de caneta USB – identificadoras de diferentes papéis no acesso à HSM), em que várias pessoas, cada uma delas possuindo uma chave PED, são obrigadas a autenticar-se antes que seja possível efetuar a cópia de segurança.

O *token hardware* de segurança com a cópia de segurança da chave privada da MULTICERT Root CA é colocado num cofre seguro em instalações seguras secundárias, e acessível apenas aos membros autorizados dos Grupos de Trabalho. O controlo de acesso físico a essas instalações impede a outras pessoas de obterem acesso não autorizado às chaves privadas.

A cópia de segurança da chave privada da MULTICERT Root CA pode ser recuperada no caso de mau funcionamento da chave original. A cerimónia de recuperação da chave utiliza os mesmos mecanismos de autenticação de dois fatores e com múltiplas pessoas, que foram utilizados na cerimónia de cópia de segurança.

7.2.3.2 Políticas e práticas de encapsulamento e recuperação de chaves de sessão

Nada a assinalar.

7.2.4 Cópia de segurança da chave privada

A chave privada da MULTICERT Root CA tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original.

Todas as chaves que tenham sido alvo de cópias de segurança, são arquivadas por um período mínimo de 30 anos após expiração da sua validade.

7.2.5 Arquivo da chave privada

As chaves privadas da MULTICERT Root CA, alvo de cópias de segurança, são arquivadas conforme identificado na secção 7.2.3.

7.2.6 Transferência da chave privada para/do módulo criptográfico

As chaves privadas da MULTICERT Root CA não são extraíveis a partir do *token* criptográfico FIPS 140-2 nível 3.

Se for realizada uma cópia de segurança das chaves privadas da MULTICERT Root CA para um outro *token* criptográfico, essa cópia é efetuada diretamente, *hardware* para *hardware*, garantindo o transporte das chaves entre módulos numa transmissão cifrada.

7.2.7 Armazenamento da chave privada no módulo criptográfico

As chaves privadas da MULTICERT Root CA são armazenadas de forma cifrada nos módulos do *hardware* criptográfico.

7.2.8 Processo para ativação da chave privada

A MULTICERT Root CA é uma EC *offline*, cuja chave privada é ativada quando o sistema da EC é ligado. Esta ativação é efetivada através da autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação de dois fatores (consola de autenticação portátil e chaves PED – pequenos *tokens* de identificação digital, com o formato de chaves físicas – identificadoras de diferentes papéis no acesso à 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 da MULTICERT Root CA é necessária, no mínimo, a intervenção de quatro elementos do Grupo de Trabalho. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

7.2.9 Processo para desativação da chave privada

A chave privada da MULTICERT Root CA é desativada quando o sistema da EC é desligado.

Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

7.2.10 Processo para destruição da chave privada

As chaves privadas da MULTICERT Root CA (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado no mínimo 30 dias após terminada a sua data de validade (ou se revogadas antes deste período).

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

7.2.11 Avaliação/nível do módulo criptográfico

Descrito na secção 7.2.1.

7.3 Outros aspetos da gestão do par de chaves

7.3.1 Arquivo da chave pública

É efetuada uma cópia de segurança de todas as chaves públicas da MULTICERT Root CA pelos membros do Grupo de Trabalho permanecendo armazenadas após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu prazo de validade.

7.3.2 Períodos de validade do certificado e das chaves

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

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

- O certificado da MULTICERT Root CA tem uma validade de 25 anos, sendo utilizado para assinar certificados durante os seus primeiros 12 anos, sendo reemitido, o mesmo, antes de atingir os 12 anos e 6 meses de validade;
- O certificado de EC subordinada da MULTICERT tem uma validade de 12 anos., sendo utilizado para assinar certificados durante os seus primeiros 6 anos de validade, sendo reemitido após os 6 anos de validade; Os certificados de OCSP (*Online Certificate Status Protocol*) têm uma validade de cinco anos e 4 meses, sendo utilizados durante os seus primeiros quatro meses de validade, sendo reemitido após o quarto mês de validade;

7.4 Dados de ativação

7.4.1 Geração e instalação dos dados de ativação

Os dados de ativação necessários para a utilização da chave privada da MULTICERT Root CA são divididos em várias partes (guardadas em chaves PED – pequenos *tokens* de identificação digital, com o formato de chaves físicas – identificadoras de diferentes papéis no acesso à HSM), ficando à responsabilidade de diferentes membros do Grupo de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves e obedecem aos requisitos definidos pela norma FIPS 140-2 nível 3.

7.4.2 Proteção dos dados de ativação

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

As chaves privadas da MULTICERT Root CA são guardadas, de forma cifrada, em *token* criptográfico.

7.4.3 Outros aspetos dos dados de ativação

Se for preciso 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.

7.5 Medidas de segurança informáticas

7.5.1 Requisitos técnicos específicos

O acesso aos servidores da MULTICERT Root CA é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. A MULTICERT Root CA tem um funcionamento *offline*, sendo desligada no fim de cada emissão de certificado ou de qualquer outra intervenção técnica necessária e que cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

7.5.2 Avaliação/nível de segurança

Os vários sistemas e produtos empregues pela MULTICERT Root CA são fiáveis e protegidos contra modificações.

O módulo criptográfico em *Hardware* da MULTICERT Root CA satisfaz a norma EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-2 nível 3.

7.6 Ciclo de vida das medidas técnicas de segurança

7.6.1 Medidas de desenvolvimento do sistema

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

É fornecida metodologia auditável que permite verificar que o *software* da MULTICERT Root CA não foi alterado antes da sua primeira utilização. Toda a configuração e alterações do *software* são executadas e auditadas por membros dos Grupos de Trabalho da PKI da MULTICERT.

7.6.2 Medidas para a gestão da segurança

A PKI da MULTICERT tem mecanismos e/ou Grupos de Trabalho, para controlar e monitorizar a configuração dos sistemas da EC. O sistema da MULTICERT Root CA, quando utilizado pela primeira vez, será verificado para garantir que o *software* utilizado é fidedigno e legal e que não foi alterado depois da sua instalação.

7.6.3 Ciclo de vida das medidas de segurança

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

7.7 Medidas de Segurança da rede

A MULTICERT Root CA, é uma EC *off-line* sendo que não se encontra ligada a nenhuma rede.

7.8 Validação cronológica (*Time-stamping*)

Certificados, LRC's e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. A informação cronológica não é baseada numa fonte de tempo dedicada. O desvio máximo é de 60 segundos. Todas as operações realizadas na MULTICERT Root CA, e sendo esta EC *offline*, iniciam-se com a verificação da data/hora do sistema.

8 Perfil de Certificado e CRL

8.1 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 do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. 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 titular.

Um certificado tem um período limitado de validade, 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.

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 ter necessidade 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 ECs assinados por outras ECs.

O perfil dos certificados emitidos pela MULTICERT Root CA está de acordo com:

- Recomendação ITU.T X.509[9];
- RFC 5280[8];
- ETSI 102 042, v2.4.1;
- ETSI 101 456, v1.4.3;
- Legislação aplicável, Nacional e Europeia.

8.2 Perfil da lista de revogação de certificados

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, várias circunstâncias 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) e, o compromisso ou suspeita de compromisso da chave privada correspondente. Sob tais circunstâncias, a EC tem que revogar 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

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

(LRC). A LRC é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LRC 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 LRC mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LRC numa base regular periódica.

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[9];
- RFC 5280[8]; e
- Legislação aplicável, Nacional e Europeia.

Os perfis das LRC podem ser consultadas nos documentos de Políticas de Certificados associadas a esta DPC, relativamente à MULTICERT Root CA (secção 3.2).

9 Auditoria de Conformidade e Outras Avaliações

Uma inspeção regular de conformidade a esta DPC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria da PKI da MULTICERT.

Para além de auditorias de conformidade, a MULTICERT irá efetuar outras fiscalizações e investigações para assegurar a conformidade da Entidades de Certificação constituintes da PKI da MULTICERT com a legislação nacional bem como com os normativos internacionais aplicáveis. A execução destas auditorias internas, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

No caso de Entidades de Certificação pertencentes à PKI da MULTICERT mas operadas por outras entidades, a MULTICERT pode, sempre que o entender, realizar auditorias internas às mesmas. Estas entidades são ainda obrigadas a, anualmente, entregar à MULTICERT o relatório de auditoria anual, ou uma declaração de conformidade, realizado por uma entidade independente e reconhecida para o efeito.

A PKI da MULTICERT está de acordo com a versão atual dos requisitos básicos para a Emissão e Gestão de Certificados *Publicly-Trusted*, publicados pelo **CA/*Browser Forum*** no documento "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*", disponibilizado em http://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.

9.1 Auditoria de Conformidade e Outras Avaliações

A MULTICERT Root CA foi auditada com sucesso e cumpre atualmente os requisitos da norma ETSI TS 102 042 e ETSI 101 456.

Esta auditoria foi desempenhada por auditores qualificados para o desempenho de auditorias relativas a esta norma, tendo estes experiência na análise de tecnologia de PKI`s, ferramentas e técnicas de segurança de informação relacionadas.

9.2 Frequência ou motivo da auditoria

As práticas de certificação da MULTICERT são alvo de auditorias periódicas, que terão como mínimo a periodicidade estipulada na lei, ou seja, uma periodicidade anual com a emissão de um relatório à data de 31 de Março do ano civil em causa. Esta auditoria será realizada por uma entidade externa registada e reconhecida para o efeito. Esta auditoria é realizada tomando como base as normas existentes para o efeito sendo os seus resultados comunicados à entidade credenciadora que poderá tornar público o resultado de todo o processo.

No sentido de cumprir com estas obrigações, a MULTICERT mantém registo de todas as operações do ciclo de vida dos certificados e de todas as comunicações mantidas com as entidades de registo/certificação por si reconhecidas. Da mesma forma, a MULTICERT obriga estas entidades a manter registo dos pedidos de subscrição recebidos e processado nos quais tenha estado envolvida.

Este registo deverá ser mantido num repositório de dados criado para o efeito e deverá poder ser confirmada através da análise dos registos das comunicações (em suporte eletrónico ou outro) com a entidade de certificação.

Para verificar o cumprimento destas disposições, a MULTICERT conduzirá auditorias periódicas sobre as entidades de registo/certificação como forma de determinar a adequação dos procedimentos operacionais e níveis de segurança tecnológicos às Políticas de Certificados suportadas. O não cumprimento das condições contratuais pode conduzir à suspensão e/ou revogação do(s) certificado(s) emitido(s).

10 Gestão da Política

10.1 Procedimento para Mudança de Especificações

10.1.1 Procedimento de Alteração à DPC

10.1.1.1 Lista de Alterações

Toda e qualquer alteração que venha a ser realizada à DPC da MULTICERT Root CA será objeto de um documento de proposta de alterações.

10.1.1.2 Mecanismo de Notificação

As alterações propostas a políticas serão colocadas na internet e comunicadas às Entidades de Registo.

10.1.1.3 Comentários

Os diversos utilizadores dos serviços prestados pela MULTICERT Root CA (subscritores, entidades de registo, de validação, de *timestamping* ou mesmo de certificação com as quais estejam estabelecidas relações de confiança mútua) poderão fazer comentários e emitir opiniões à MULTICERT ou às Entidades de Registo.

10.1.1.4 Mecanismos para tratar Comentários

Uma vez compilados os comentários será apresentada uma proposta de alterações formal ao Grupo de Gestão da PKI da MULTICERT, devidamente acompanhada dos comentários recolhidos. O Grupo de Gestão terá como obrigação fazer o pedido de um parecer à Autoridade Credenciadora sobre o impacto destas alterações na credenciação da MULTICERT Root CA.

Uma vez na posse de toda esta informação, o Grupo de Gestão e o Grupo de Trabalho deAutenticação deliberarão em relação ao provimento das propostas de alteração da DPC, devendo proceder-se à notificação de todos os interessados sobre as deliberações tomadas. Os subscritores terão então um período máximo de 30 dias para solicitar a rescisão de contrato com a MULTICERT Root CA, sem o qual se tomarão como aceites as novas disposições.

10.1.1.5 Período de Entrada em efeito das Alterações

Após este processo ser concluído as alterações passarão à prática após 30 dias. Serão adotados mecanismos de controlo para garantir que todas as alterações às PC`s e à DPC são rasteadas e que é adotado um correto mecanismo de controlo de versões.

10.2 Políticas de Publicação e Notificação

10.2.1 Requerimento de Publicação e Notificação

Todos os itens constantes das PC`s e da DPC da MULTICERT Root CA estão sujeitos a publicação e notificação.

Toda a publicação e notificação será feita através do *site* da MULTICERT (https://pki.multicert.com/index.html), a não ser que a notificação tenha grande impacto para a MULTICERT e para os seus clientes.

A MULTICERT Root CA pode assinar digitalmente cada publicação e cada notificação antes de estas serem colocadas no respetivo *site*.

A MULTICERT disponibilizará, publicará ou notificará os seus clientes acerca de:

- Formas adequadas de proteção de chaves privadas;
- Riscos associados ao uso de qualquer certificado emitido pela MULTICERT Root CA cuja tecnologia tenha sido descontinuada.

10.2.2 Publicação da DPC Atualizada

O documento de DPC, devidamente atualizado deverá estar permanentemente disponível através do URL https://pki.multicert.com/index.html.

10.2.3 Procedimento de Aprovação da DPC

A validação desta DPC (e/ou respetivas PC`s) e seguintes correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Autenticação. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetivas PC`s), substituindo qualquer DPC (e/ou respetivas PC`s) anteriormente definida. O Grupo de Trabalho de Autenticação deverá ainda determinar quando é que as alterações na DPC (e/ou respetivas PC`s) levam a uma alteração nos identificadores dos objetos (OID) da DPC (e/ou respetivas PC`s).

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

11 OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

Esta secção aborda aspetos de negócio e assuntos legais.

11.1 Taxas

11.1.1 Taxas por emissão ou renovação de certificados

A serem identificadas em proposta formal a efetuar pela MULTICERT.

11.1.2 Taxas para acesso a certificado

Nada a assinalar.

11.1.3 Taxas para acesso a informação do estado do certificado ou de revogação

O acesso a informação sobre o estado ou revogação dos certificados (LRC) é livre e gratuita.

11.1.4 Taxas para outros serviços

As taxas para os serviços de validação cronológica e validação *online* OCSP são identificadas em proposta formal a efetuar pela MULTICERT.

11.1.5 Política de reembolso

Nada a assinalar.

11.2 Responsabilidade financeira

11.2.1 Seguro de cobertura

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

11.2.2 Outros recursos

Nada a assinalar.

11.2.3 Seguro ou garantia de cobertura para utilizadores

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

11.3 Confidencialidade da informação processada

11.3.1 Âmbito da confidencialidade da informação

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

a) As chaves privadas da MULTICERT Root CA;

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

c) Toda a informação de carácter pessoal proporcionada à PKI da MULTICERT durante o processo de registo dos subscritores de certificados, salvo se houver autorização explicita para a sua divulgação e/ou se a mesma não for incluída no conteúdo do certificado emitido;

d) Planos de continuidade de negócio e recuperação;

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

f) Informação de todos os documentos relacionados com a PKI da 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 da 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;

g) Todas as palavras-chave, PIN`s e outros elementos de segurança relacionados com a MULTICERT Root CA;

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

i) A localização dos ambientes da PKI da MULTICERT e seus conteúdos.

11.3.2 Informação fora do âmbito da confidencialidade da informação

Considera-se informação de acesso público:

a) Política de Certificados;

b) Declaração de Práticas de Certificação;

c) LCR e,

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

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

11.3.3 Responsabilidade de proteção da confidencialidade da informação

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

11.4 Privacidade dos dados pessoais

11.4.1 Medidas para garantia da privacidade

O Sistema de Gestão de Ciclo de Vida dos Certificados (SGCVC) é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa.

11.4.2 Informação privada

É considerada informação privada toda a informação fornecida pelo titular do certificado que não seja disponibilizada no certificado digital do titular.

11.4.3 Informação não protegida pela privacidade

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

11.4.4 Responsabilidade de proteção da informação privada

De acordo com a legislação portuguesa.

11.4.5 Notificação e consentimento para utilização de informação privada

De acordo com a legislação portuguesa.

11.4.6 Divulgação resultante de processo judicial ou administrativo

Nada a assinalar.

11.4.7 Outras circunstâncias para revelação de informação

Nada a assinalar.

11.5 Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados, LCR e Delta-LRC emitidos, OID, DPC e PC, bem como qualquer outro documento, propriedade da PKI da MULTICERT pertence à MULTICERT S.A..

As chaves privadas e as chaves públicas são propriedade do titular, independentemente do meio físico que se empregue para o seu armazenamento.

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

11.6 Representações e garantias

11.6.1 Representação e garantias das entidades certificadoras

A PKI da MULTICERT está obrigada a:

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

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 de sua emissão e livres de erros de entrada de dados;

f) Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;

g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;

h) Utilizar sistemas fiáveis para armazenar certificados reconhecidos que permitam comprovar a sua autenticidade e impedir que pessoas não autorizadas alterem os dados;

i) Arquivar sem alteração os certificados emitidos;

j) Garantir que podem determinar com precisão da data e hora em que emitiu ou extinguiu ou suspendeu um certificado;

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

l) Revogar os certificados nos termos da secção 5.7 deste documento e publicar os certificados revogados na LRC do repositório da MULTICERT Root CA, com a frequência estipulada na secção 5.7.10;

m) Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;

n) Notificar com a rapidez necessária, por correio eletrónico os titulares dos certificados em caso da EC proceder à revogação ou suspensão dos mesmos, indicando o motivo que originou esta ação;

o) Colaborar com as auditorias dirigidas pela Autoridade Credenciadora, para validar a renovação das suas próprias chaves;

p) Operar de acordo com a legislação aplicável;

q) Proteger em caso de existirem as chaves que estejam sobre sua custódia;

r) Garantir a disponibilidade da LRC de acordo com as disposições da secção 5.7.10;

s) Em caso de cessar a sua atividade deverá comunicar com uma antecedência mínima de dois meses a todos os titulares dos certificados emitidos assim como à Autoridade Credenciadora;

t) Cumprir com as especificações contidas na norma sobre Proteção de Dados Pessoais;

u) Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante quinze anos desde o momento da emissão e,

v) Disponibilizar os certificados da MULTICERT Root CA.

11.6.2 Representação e garantias das Entidades de Registo

Nada a assinalar.

11.6.3 Representação e garantias dos titulares

É obrigação dos titulares dos certificados emitidos:

a) Limitar e adequar a utilização dos certificados de acordo com as utilizações previstas nas Politicas de Certificado;

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 de compromisso da chave privada correspondente à chave pública contida no certificado, de acordo com a secção 5.7.5;

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

e) Submeter às Entidade de Certificação (ou de Registo) a informação que considerem exata e completa com relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação e,

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

11.6.4 Representação e garantias das partes confiantes

É obrigação das partes que confiem nos certificados emitidos pela PKI da MULTICERT:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na Politica de Certificado correspondente;

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

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

d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que 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.

11.6.5 Representação e garantias de outros participantes

Nada a assinalar.

11.7 Renúncia de garantias

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

11.8 Limitações às obrigações

A MULTICERT Root CA:

a) Responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Artº 26 do DL 62/2003;

b) Responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele;

c) Assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação;

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

e) Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso;

f) Não responde quando o titular superar os limites que figuram no certificado quanto as suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular;

g) Não assume qualquer responsabilidade no caso de perca ou prejuízo:

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

   iii) Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Politica de Certificados e correspondente DPC;

   iv) Ocasionado pelo uso indevido ou fraudulento dos certificados ou CRL emitidos pela MULTICERT Root CA.

11.9 Indemnizações

De acordo com a legislação em vigor.

11.10 Termo e cessação da atividade

11.10.1 Termo

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

Esta DPC entra em vigor desde o momento de sua publicação no repositório da MULTICERT Root CA.

Esta DPC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão ou pela renovação das chaves da MULTICERT Root CA, momento em que obrigatoriamente se redigirá uma nova versão.

11.10.2 Substituição e revogação da DPC

O Grupo de Trabalho de Gestão pode decidir em favor da eliminação ou emenda de um documento relacionado com a PKI da MULTICERT (incluindo esta DPC) quando:

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

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

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

Quando a DPC ficar revogada será retirada do repositório público, garantindo-se contudo que será conservada durante 20 anos.

11.10.3 Consequências da cessação de atividade

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

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

11.11 Notificação individual e comunicação aos participantes

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

11.12 Alterações

11.12.1 Procedimento para alterações

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

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

O Grupo de Trabalho de Autenticação vai rever o pedido feito e, se verificar a sua pertinência, procede às atualizações necessárias ao documento, resultando numa nova versão de rascunho do documento. O novo rascunho do documento é depois disponibilizado a todos os membros do Grupo de Trabalho e às partes afetadas (se alguma) para permitir o seu escrutínio. Contando a partir da data de disponibilização, as várias partes têm 15 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Trabalho de Autenticação tem mais 15 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento, após o que o documento é aprovado e fornecido Grupo de Trabalho de Gestão para validação, aprovação e publicação, tornando-se as alterações finais e efetivas.

11.12.2 Prazo e mecanismo de notificação

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

11.12.3 Motivos para mudar de OID

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

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

No caso em que o Grupo de Trabalho de Autenticação julgue que as alterações à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 11.12.2.

11.13 Disposições para resolução de conflitos

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

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

11.14 Legislação aplicável

É aplicável à atividade das entidades certificadoras a seguinte legislação específica:

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

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

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

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

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

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

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

h) ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI): policy requirements for certification authorities issuing public key certificates, v2.4.1.

i) ETSI TS 101 456: Electronic Signatures and infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, v1.4.3.

j) CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.0

11.15 Conformidade com a legislação em vigor

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

É responsabilidade da Autoridade Credenciadora zelar pelo cumprimento da legislação aplicável listada na secção 11.14.

11.16 Providências várias

11.16.1 Acordo completo

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

11.16.2 Independência

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

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

11.16.3 Severidade

Nada a assinalar.

11.16.4 Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

11.16.5 Força Maior

Nada a assinalar.

11.17 Outras providências

Nada a assinalar.

12 Lista de Definições e Acrónimos

Definições

Assinatura digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura eletrónica	Resultado de um processamento eletrónico de dados, suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Assinatura eletrónica avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade Credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado	Certificado que contém os elementos referidos no artigo 29.º do DL 62/2003 [7] e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24.º do DL 62/2003.
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado

	com a correspondente chave pública.
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos.
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica.
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) 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) 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) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Estampilha temporal	Estrutura de dados que liga a representação eletrónica de um *datum* com uma data/hora particular, estabelecendo evidência de que o *datum* existia nessa data/hora.
Parte confiante	Recetor de uma estampilha temporal que confia na mesma.
Sistema TSA (*TSA system*)	Composição de produtos IT e componentes, organizados de modo a

	suportar o fornecimento de serviços de validação cronológica.
UTC (*Coordinated Universal Time*)	Escala de tempo baseada no segundo, como definido na *ITU-R Recommendation TF.460-5* [10].
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1* [11])
Validação cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.

Acrónimos

ANS	*Autoridade Nacional de Segurança*
ANSI	*American National Standards Institute*
C	*Country*
CA	*Certification Authority* (o mesmo que EC)
CN	*Common Name*
CRL	Ver LRC
DL	Decreto Lei
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
DR	Decreto Regulamentar
EC	Entidade de Certificação
ECD	Entidade Certificadora de Documentos
ER	Entidade de Registo
GMT	Tempo Médio de Greenwich (*Greenwich Mean Time*)
LRC	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
O	*Organization*
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objecto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infra-estrutura de Chave Pública)
SHA	*Secure Hash Algorithm*
SGCVC	*Sistema de Gestão de Ciclo de Vida de Certificados*
SSCD	*Secure Signature-Creation Device*
TSA	*Time-Stamping Authority* (o mesmo que EVC)

Aprovação

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

Assinado de forma digital por [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
DN: c=PT, o=MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A., ou=Certificado para pessoa colectiva - Assinatura Qualificada, title=Procurador com poderes indicados na procuração emitida em 16/10/2013 - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, serialNumber=505767457, cn=[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA, S.A.
Dados: 2015.10.08 14:52:00 +01'00'