Declaração de Práticas de Certificação

Políticas

MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf

Identificação do Projecto: MULTICERT CA03

Identificação da CA: MULTICERT CA

Nível de Acesso: Público

Versão: 1.0

Data: 28/12/2008

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Estrada Casal de Canas, Lote 6 – Alfragide, Amadora, 2720-092 Portugal
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

Identificador do documento: MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf

Palavras-chave: EC MULTICERT, Declaracao de Praticas de Certificacao

Tipologia documental: Políticas

Título: Declaração de Práticas de Certificação

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 28/12/2008

Versão actual: 1.0

Identificação do Projecto: MULTICERT CA03

Identificação da CA: MULTICERT CA

Cliente: MULTICERT S.A.

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	28/12/2008	Versão inicial	José Pina Miranda

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.2_0001_pt.pdf	Politica de Certificado da raiz auto-assinada da EC MULTICERT	José Pina Miranda
MULTICERT_PJ.CA3_24.1.2_0002_pt.pdf	Politica de Certificado de Assinatura Digital Qualificada	José Pina Miranda
MULTICERT_PJ.CA3_24.1.2_0003_pt.pdf	Politica de Certificado de Autenticação	José Pina Miranda

Resumo Executivo

Decorrente da implementação de vários programas públicos e privados para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não governamentais e o Estado, com vista ao fortalecimento da sociedade de informação, do governo electrónico (*eGovernment*) e do comércio electrónico, os certificados digitais emitidos pela Entidade de Certificação MULTICERT, registada junto da Autoridade Credenciadora (conforme previsto na legislação europeia e nacional), fornecem os mecanismos necessários para a autenticação digital forte da identidade do titular do certificado electrónico, assim como as assinaturas electrónicas (equivalente legal das assinaturas manuscritas) indispensáveis aos processos de desmaterialização.

A infra-estrutura da Entidade de Certificação MULTICERT fornece uma hierarquia de confiança, que promove a segurança electrónica do titular do certificado digital. A Entidade de Certificação MULTICERT estabelece uma estrutura de confiança electrónica que proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

A Entidade de Certificação MULTICERT está devidamente registada junto da Autoridade Nacional de Segurança (http://www.gns.gov.pt/gns/pt/assinatura/), 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).

Este documento define os procedimentos e práticas utilizadas pela Entidade de Certificação MULTICERT no suporte à sua actividade de certificação digital, sendo referenciado como o documento de Declaração de Práticas de Certificação da Entidade de Certificação MULTICERT.

Sumário

Introdução

Objectivos

O objectivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Certificação MULTICERT (EC MULTICERT) no suporte à sua actividade de certificação digital.

Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC MULTICERT,
- Terceiras partes encarregues de auditar a EC MULTICERT,
- Todo o público, em geral.

Estrutura do Documento

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

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

Os primeiros oito capítulos são dedicados a descrever os procedimentos e práticas mais importantes no âmbito da certificação digital da EC MULTICERT. O capítulo oito descreve auditorias de conformidade e outras avaliações. O capítulo nove descreve matérias legais.

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

1 Introdução

O presente documento é uma Declaração de Práticas de Certificação, ou DPC, cujo objectivo se prende com a definição de um conjunto de práticas para a emissão e validação de Certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações, mas antes informar pelo que se pretende que este documento seja simples, directo 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 MULTICERT (EC MULTICERT) e, explica o que um Certificado fornece e significa, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos Certificados emitidos pela EC MULTICERT. Este documento pode sofrer actualizações regulares.

Os Certificados emitidos pela EC MULTICERT contêm uma referência ao DPC de modo a permitir que Partes confiantes e outras pessoas interessadas possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

A Entidade de Certificação MULTICERT é detida pela empresa MULTICERT – Serviços de Certificação Electrónica, S.A.

1.1 Visão Geral

As práticas de criação, assinatura e de 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 infra-estrutura de Chaves Públicas ("*PKI – Public Key Infrastructure*").

Este DPC aplica-se especificamente à EC MULTICERT e respeita e implementa os seguintes standards:

- *RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*,
- *RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

1.2 Designação e Identificação do Documento

Este documento é a Declaração de Práticas de Certificação da EC MULTICERT. A DPC é representada num certificado através de um número único designado de "identificador de objecto" (OID), sendo o valor do OID associado a este documento o 1.3.6.1.4.1.25070.1.1.1.0.7. O OID da Política de Certificado é utilizado de acordo com o explicitado na secção 7.1.6.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.0.7
Data de Emissão	21/Janeiro/2009

Validade	Não aplicável
Localização	http://pki.multicert.com/pol/cps/MULTICERT_CA.html

1.3 Participantes na Infra-Estrutura de Chave Pública

1.3.1 Entidades Certificadoras

A EC MULTICERT é uma entidade certificadora registada junto da Autoridade Nacional de Segurança (http://www.gns.gov.pt/gns/pt/assinatura/), 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 hierarquia 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 EC MULTICERT é reconhecida na maioria dos sistemas operativos e navegadores Web, sendo a sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores.

A EC MULTICERT emite certificados de:

- Assinatura Qualificada para pessoa singular,
- Assinatura Qualificada para pessoa colectiva,
- Autenticação para pessoa singular,
- Autenticação para pessoa colectiva,
- serviços da PKI MULTICERT, i.e., certificados para serviços necessários no âmbito da EC MULTICERT:
    - validação on-line OCSP,
    - validação cronológica.

1.3.2 Entidades de Registo

Não existem entidades de registo. Os serviços internos da Entidade de Certificação MULTICERT procedem ao registo e validação dos dados necessários, conforme explicitado na Politica de Certificado de cada tipo de certificados emitidos.

1.3.3 Titulares de certificados

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados pela EC MULTICERT.

São considerados titulares de certificados emitidos pela EC MULTICERT, aqueles cujo nome está inscrito no campo "Assunto" (*Subject)* do certificado e utilizam o certificado e respectiva chave privada de acordo com o estabelecido nas diversas politicas de certificado descritas neste documento, sendo emitidos certificados para as seguintes categorias titulares:

- Pessoa singular – certificados de Autenticação e Assinatura Qualificada;
- Pessoa colectiva – certificados de Autenticação e Assinatura Qualificada;
- Equipamentos tecnológicos – certificados de validação on-line OCSP, validação cronológica.

1.3.3.1 Patrocinador

A emissão de certificados para equipamentos tecnológicos (p.e: computadores, firewall, routers, servidores, etc.) é efectuada sempre sob responsabilidade humana, sendo esta entidade designada por patrocinador.
O patrocinador aceita o certificado e é responsável pela sua correcta utilização, bem como pela protecção e salvaguarda da sua chave privada.

1.3.4 Partes Confiantes

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

Nesta DPC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido pela EC MULTICERT.

1.3.5 Outros participantes

1.3.5.1 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/inspecção de conformidade, no sentido de aferir se os processos utilizados pelas EC nas suas actividades 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:

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

b) Registo: procedimento sem o qual a EC não poderá emitir os Certificados Qualificados;

c) Fiscalização: procedimento assente em inspecções efectuadas às EC, com vista a regularmente verificar parâmetros de conformidade;

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

1.3.5.2 Entidade de Validação OCSP

As Entidades de Validação OCSP, têm como função comprovar o estado dos certificados emitidos, através da utilização do protocolo *Online Certificate Status Protocol*[2] (OCSP), de forma a determinar o estado actual do certificado a pedido de uma entidade sem necessidade de recorrer à verificação do estado através da consulta das Listas de Certificados Revogados (LCR).
O serviço de Entidade de Validação OCSP é disponibilizado pela EC MULTICERT.

1.3.5.3 Entidade de Validação Cronológica

As Entidades de Validação cronológica emitem declarações electrónicas que atestam a data e hora da criação, expedição ou recepção de um documento electrónico.
O serviço de Entidade de Validação Cronológica é disponibilizado pela EC MULTICERT.

1.3.5.4 Auditor de Segurança

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

A EC MULTICERT promove uma política de rotação dos seus auditores de seguranças, tal como as melhores práticas prevêem. Os auditores de segurança da EC MULTICERT foram/são os seguintes:

NOME	Data início – Data de fim
Paulo Jorge Martins Borges	15/Dez/2008 –

1.4 Utilização do Certificado

Os certificados emitidos no domínio da EC MULTICERT são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objectivo 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 EC 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.

1.4.1 Utilização adequada

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

[2] *cf.* RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

Os certificados emitidos para equipamentos tecnológicos, têm como objectivo 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 o grau de RESERVADO 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 pela EC MULTICERT são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob a EC 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 EC MULTICERT.

1.4.2 Utilização não autorizada

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pela legislação aplicável.
Os certificados emitidos pela EC MULTICERT não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.
Os serviços de certificação oferecidos pela EC MULTICERT, não foram desenhados nem estão autorizados a ser utilizados em actividades de alto risco ou que requeiram um actividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra actividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

1.5 Gestão das Políticas

1.5.1 Entidade responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do Grupo de Políticas da EC MULTICERT.

1.5.2 Contacto

NOME	Grupo de Políticas da EC MULTICERT
Gestor:	Sara Loja
Morada:	MULTICERT S.A. Estrada Casal de Canas, Lote 6 Alfragide 2720-092 Amadora, Portugal
Correio electrónico:	grupo_politicas@multicert.com
Página Internet:	www.multicert.com
Telefone:	+351 217 123 010
Fax:	+351 217 123 011

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

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

1.5.4 Procedimentos para Aprovação da DPC

A validação desta DPC (e/ou respectivas PCs) e seguintes correcções (ou actualizações) deverão ser levadas a cabo pelo Grupo de Políticas. Correcções (ou actualizações) deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respectivas PCs), substituindo qualquer DPC (e/ou respectivas PCs) anteriormente definida. O Grupo de Políticas deverá ainda determinar quando é que as alterações na DPC (e/ou respectivas PCs) levam a uma alteração nos identificadores dos objectos (OID) da DPC (e/ou respectivas PCs) .
Após a fase de validação, a DPC (e/ou respectivas PCs) é submetida ao Grupo de Gestão, que é a entidade responsável pela aprovação e autorização de modificações neste tipo de documentos.

1.6 Definições e acrónimos

1.6.1 Acrónimos

Acrónimo	
ANSI	*American National Standards Institute*
CA	*Certification Authority* (o mesmo que EC)
CRL	Ver LRC
DL	Decreto Lei
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EAL	*Evaluation Assurance Level*
EC	Entidade de Certificação
LRC	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objecto

PC	Politica de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infra-estrutura de chave Pública)
SGCVC	Sistema de Gestão do Ciclo de Vida dos Certificados
SSCD	Secure Signature-Creation Device

1.6.2 Definições

Definição	
Assinatura digital	Modalidade de assinatura electrónica 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 electrónico 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 electrónico foi alterado depois de aposta a assinatura.
Assinatura electrónica	Resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico.
Assinatura electrónica avançada	Assinatura electrónica 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 detectar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura electrónica qualificada	Assinatura digital ou outra modalidade de assinatura electrónica 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 electrónico 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 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 electrónico, ou se decifra um documento electrónico 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 electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Acto pelo qual é reconhecido a uma entidade que o solicite e que exerça a actividade 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 electrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura electrónica.
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 electrónico	Documento elaborado mediante processamento electrónico de dados.
Endereço electrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos

	electrónicos.
Entidade certificadora	Entidade ou pessoa singular ou colectiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respectiva publicidade e presta outros serviços relativos a assinaturas electrónicas.
Organismo de certificação	Entidade pública ou privada competente para a avaliação e certificação da conformidade dos processos, sistemas e produtos de assinatura electrónica com os requisitos a que se refere a alínea c) do n.º 1 do artigo 12.º do DL 62/2003.
Produto de assinatura electrónica	Suporte lógico, dispositivo de equipamento ou seus componentes específicos, destinados a ser utilizados na prestação de serviços de assinatura electrónica qualificada por uma entidade certificadora ou na criação e verificação de assinatura electrónica qualificada.
Titular	Pessoa singular ou colectiva identificada num certificado como a detentora de um dispositivo de criação de assinatura.
Validação cronológica	Declaração de entidade certificadora que atesta a data e hora da criação, expedição ou recepção de um documento electrónico.

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

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

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

- disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efectuadas em horário de menor utilização, garantindo-se durante o tempo da disponibilidade:
    - 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 efectuado através do protocolo HTTPS e HTTP, estando implementado os seguintes mecanismos de segurança:

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

2.2 Publicação de informação de certificação

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

O Ministério da Justiça disponibiliza sempre a seguinte informação pública on-line:

- cópia electrónica deste DPC e Políticas de Certificados (PC) mais actuais da EC MULTICERT, assinada electronicamente, por individuo devidamente autorizado e com certificado digital atribuído para o efeito:
    - DPC da EC MULTICERT disponibilizada no URI: http://pki.multicert.com/pol/cps/MULTICERT_CA.html ,
    - PC de certificado auto-assinado da EC MULTICERT disponibilizada no URI: http://pki.multicert.com/pol/cp/root.html ,
    - PC de certificado de Validação on-line OCSP disponibilizada no URI: http://pki.multicert.com/pol/cp/ocsp.html,

  - PC de certificado de Validação Cronológica disponibilizada no URI: http://pki.multicert.com/pol/cp/timestamp.html,
  - PC de certificado de autenticação disponibilizada no URI: http://pki.multicert.com/pol/cp/auth.html ,
  - PC de certificado de assinatura digital qualificada disponibilizada no URI: http://pki.multicert.com/pol/cp/adq.html .

- LRC da EC MULTICERT – URI: http://pki.multicert.comt/crl/crl<ID_CA>.crl ;
- Delta-LRC da EC MULTICERT – URI: http://pki.multicert.com/crl/crl<ID_CA>_delta.crl ;
- certificado da EC MULTICERT – URI: http://pki.multicert.com/cert/MULTICERT_CA ;
- outra informação relevante – URI: http://pki.multicert.com/info/MULTICERT_CA .

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

2.3 Periodicidade de publicação

As actualizações a esta DPC e respectivas PC serão publicadas imediatamente após a sua aprovação pelo Grupo de Gestão, de acordo com a secção 9.12.

O certificado da EC MULTICERT é publicado imediatamente após a emissão. A LRC da EC MULTICERT será publicada, no mínimo, uma vez por semana. A Delta-LRC da EC MULTICERT será publicada, no mínimo, todos os dias.

2.4 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.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Atribuição de Nomes

A atribuição de nomes segue a seguinte convenção:

- aos certificados de pessoa singular é atribuído o nome real do titular (ou pseudónimo),
- aos certificados de equipamentos tecnológicos é atribuído o nome qualificado do domínio e/ou o âmbito da sua utilização.

3.1.1 Tipos de nomes

O certificado da EC MULTICERT assim com os certificados emitidos pela EC MULTICERT são identificados por um nome único (DN – Distinguished Name) de acordo com standard X.500.

O nome único destes certificados está identificado nas respectivas Políticas de Certificados:

Tipo de Certificado	OID da Política de Certificados
EC MULTICERT (raiz auto-assinada)	1.3.6.1.4.1.25070.1.1.1.1.0.1.1
Validação on-line OCSP	1.3.6.1.4.1.25070.1.1.1.1.0.1.4
Validação cronológica	1.3.6.1.4.1.25070.1.1.1.1.0.1.5
Autenticação	1.3.6.1.4.1.25070.1.1.1.1.0.1.3
Assinatura Digital Qualificada	1.3.6.1.4.1.25070.1.1.1.1.0.1.2

3.1.2 Necessidade de nomes significativos

A EC MULTICERT irá assegurar, dentro da sua hierarquia de confiança:

- a não existência de certificados que, tendo o mesmo nome único identifiquem entidades distintas,
- a relação entre o titular e a organização a que pertence é a mesma que consta no certificado e é facilmente perceptível e identificável pelos Humanos (com excepção dos certificados com pseudónimos).

3.1.3 Anonimato ou pseudónimo de titulares

A EC MULTICERT emite certificados com pseudónimo de titulares, garantindo para o efeito que:

- o certificado contém o pseudónimo do titular, claramente identificado como tal,
- conserva os elementos que comprovam a verdadeira identidade dos requerentes titulares de certificados com pseudónimo,

- comunicará à autoridade judiciária, sempre que esta o ordenar nos termos legalmente previstos, os dados relativos à identidade dos titulares de certificados que sejam emitidos com pseudónimo seguindo-se, no aplicável, o regime do artigo 182.º do Código de Processo Penal.

3.1.4 Interpretação de formato de nomes

As regras utilizadas pela EC MULTICERT para interpretar o formato dos nomes seguem o estabelecido no RFC 5280[3], assegurando que todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado são codificados numa *UTF8String*, com excepção dos atributos *country* e *serialnumber* que são codificados numa *PrintableString*.

3.1.5 Unicidade de nomes

Os identificadores do tipo DN são únicos para cada titular de certificado emitido dentro da EC MULTICERT, não induzindo em ambiguidades.

De acordo com os seus processos de emissão, a EC MULTICERT rejeita a emissão de certificados com o mesmo DN para titulares distintos. Para cada tipo de certificado emitido, a respectiva Política de Certificados indica o conteúdo do *serialnumber* que deverá ser escolhido de modo a assegurar a unicidade do campo e a não induzir uma parte confiante em ambiguidade.

3.1.6 Reconhecimento, autenticação, e função das marcas registadas

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

No procedimento de autenticação e identificação do titular do certificado, prévio à emissão do mesmo, a entidade requisitante do certificado terá que apresentar os documentos legais que demonstrem o direito à utilização do nome requisitado.

3.2 Validação de Identidade no registo inicial

Para cada tipo de certificados, a respectiva Política de Certificado descreve todos os passos necessários, desde o início do pedido de certificado até à atribuição do certificado digital ao seu titular.

3.3 Identificação e Autenticação para pedidos de renovação de chaves

A identificação e autenticação para a renovação de certificados são realizadas utilizando os procedimentos para a autenticação e identificação inicial (cf. secção 3.2).

3.3.1 Identificação e autenticação para renovação de chaves, de rotina

Não existe renovação de chaves, de rotina. A renovação de certificados utiliza os procedimentos para a autenticação e identificação inicial, onde são gerados novos pares de chaves.

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

3.3.2 Identificação e autenticação para renovação de chaves, após revogação

Após revogação de certificado, a geração de novo par de chaves e respectiva emissão de certificado segue os procedimentos para a autenticação e identificação inicial.

3.4 Identificação e autenticação para pedido de revogação

Para cada tipo de certificados, a respectiva Política de Certificado descreve o modo de identificação e autenticação para pedido de revogação.

4 Requisitos operacionais do ciclo de vida do certificado

4.1 Pedido de Certificado

Para cada tipo de certificados, a respectiva Política de Certificado descreve o pedido de certificado.

4.2 Processamento do pedido de certificado

Para cada tipo de certificados, a respectiva Política de Certificado descreve o modo de processamento do pedido de certificado.

4.3 Emissão de Certificado

Para cada tipo de certificados, a respectiva Política de Certificado descreve a emissão de certificado.

4.4 Aceitação do Certificado

Para cada tipo de certificados, a respectiva Política de Certificado descreve o modo de aceitação do Certificado.

4.5 Uso do certificado e par de chaves

Para cada tipo de certificados, a respectiva Política de Certificado descreve o uso do certificado e par de chaves.

4.6 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 excepção do período de validade do certificado.

Esta prática não é suportada na EC MULTICERT.

4.6.1 Motivos para renovação de certificado

Nada a assinalar.

4.6.2 Quem pode submeter o pedido de renovação de certificado

Nada a assinalar.

4.6.3 Processamento do pedido de renovação de certificado

Nada a assinalar.

4.6.4 Notificação de emissão de novo certificado ao titular

Nada a assinalar.

4.6.5 Procedimentos para aceitação de certificado

Nada a assinalar.

4.6.6 Publicação de certificado após renovação

Nada a assinalar.

4.6.7 Notificação da emissão do certificado a outras entidades

Nada a assinalar.

4.7 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 (ou patrocinador) 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 SCEE, é designado por renovação de certificado com geração de novo par de chaves.

Para cada tipo de certificados, a respectiva Política de Certificado descreve a renovação de certificado com geração de novo par de chaves.

4.8 Modificação de certificados

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

Esta prática não é suportada pela EC MULTICERT.

4.8.1 Motivos para alteração do certificado

Nada a assinalar.

4.8.2 Quem pode submeter o pedido de alteração de certificado

Nada a assinalar.

4.8.3 Processamento do pedido de alteração de certificado

Nada a assinalar.

4.8.4 Notificação da emissão de certificado alterado ao titular

Nada a assinalar.

4.8.5 Procedimentos para aceitação de certificado alterado

Nada a assinalar.

4.8.6 Publicação do certificado alterado

Nada a assinalar.

4.8.7 Notificação da emissão de certificado alterado a outras entidades

Nada a assinalar.

4.9 Suspensão e revogação de certificado

Na prática, a revogação e suspensão de certificados é uma acção através da qual o certificado deixa de estar válido antes do fim do seu período de validade, perdendo a sua operacionalidade.

Os certificados depois de revogados não podem voltar a ser válidos, enquanto que os certificados suspensos podem recuperar a sua validade.

Para cada tipo de certificados, a respectiva Política de Certificado descreve a suspensão e revogação de certificado.

4.10 Serviços sobre o estado do certificado

4.10.1 Características operacionais

O estado dos certificados emitidos está disponível publicamente através das LCR e Delta-LCR.

4.10.2 Disponibilidade do serviço

O Serviço sobre o estado do certificado está disponível 24 horas por dia, 7 dias por semana, excepto para paragens de manutenção programadas.

4.10.3 Características opcionais

Nada a assinalar.

4.11 Fim de subscrição

O fim da operacionalidade de um certificado acontece quando se verificarem uma das seguintes situações:

a) revogação do certificado;

b) por ter caducado o prazo de validade do certificado.

4.12 Retenção e recuperação de chaves (Key escrow)

A EC MULTICERT só efectua a retenção da sua chave privada.

4.12.1 Políticas e práticas de recuperação de chaves

A chave privada da EC MULTICERT é armazenada num *token* hardware de segurança, sendo efectuada uma cópia de segurança utilizando uma ligação directa 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 EC MULTICERT.

A cerimónia de cópia de segurança utiliza um HSM com autenticação de dois factores (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 efectuar a cópia de segurança.

O *token* hardware de segurança com a cópia de segurança da chave privada da EC MULTICERT 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 EC MULTICERT 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 factores e com múltiplas pessoas, que foram utilizados na cerimónia de cópia de segurança.

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

Nada a assinalar.

5 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 desta DPC. Esta secção descreve sucintamente os aspectos 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 EC.

5.1 Medidas de segurança física

5.1.1 Localização física e tipo de construção

As instalações da EC 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 arquitectura 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 EC 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, detecta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

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

a) Paredes em alvenaria, betão ou tijolo;

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

c) Inexistência de janelas;

d) Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança accionável electronicamente, características corta – fogo e funcionalidade antipânico.

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

- Perímetros de segurança claramente definidos;
- Paredes, chão e tecto em alvenaria, sem janelas, que impedem acessos não autorizados;
- Trancas e fechaduras anti roubo de alta segurança nas portas de acesso ao ambiente de segurança.
- O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;
- Acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

5.1.2 Acesso físico ao local

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

Actividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer actividades 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. A 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 respectivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respectivo cartão de acesso visível.

O acesso à zona mais restrita de alta segurança requer controlo duplo, cada um deles utilizando dois factores de autenticação, incluindo autenticação biométrica. O hardware criptográfico e *tokens* físicos seguros dispõem de protecção adicional, sendo guardados em cofres e armários seguros. O acesso à zona mais restrita de alta segurança, assim como ao hardware criptográfico e aos *tokens* físicos seguros é restrito, de acordo com as necessidades de segregação de responsabilidades dos vários Grupos de Trabalho.

5.1.3 Energia e ar condicionado

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

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

5.1.4 Exposição à água

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

5.1.5 Prevenção e protecção contra incêndio

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

- sistemas de detecção 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.

5.1.6 Salvaguarda de suportes de armazenamento

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

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

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

5.1.7 Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível 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 respectivo fabricante, antes da sua eliminação. Outros equipamentos de armazenamento (discos rígidos, tapes,...) deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

5.1.8 Instalações externas (alternativa) para recuperação de segurança

Todas as cópias de segurança são guardados em ambiente seguro em instalações externas, ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir o acesso apenas a pessoal autorizado, garantindo também a protecção contra danos acidentais (e.g., causados por água ou fogo).

5.2 Medida de segurança dos processos

A actividade de uma Entidade Certificadora 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.

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

5.2.1 Grupos de Trabalho

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

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

5.2.1.1 Grupo de Trabalho de Instalação

É responsável pela instalação e configuração de base (*hardware* e *software*) da EC até à sua inicialização. Este grupo deve ter pelo menos 1 (um) membro.

As responsabilidades deste grupo são:

- Instalar, interligar e configurar o *hardware* da EC;
- Instalar e configurar o *software* de base da EC;
- Configurar as palavras-passe iniciais necessárias[4], que irão ser alteradas posteriormente pelo Grupo de Trabalho de Autenticação;
- Preparar comunicados sobre:
    - As palavras-passe iniciais;
    - Identificação dos membros do Grupo de Trabalho de Instalação;
    - *Hash* do(s) CD(s) de instalação utilizados;
    - A lista de todos os artefactos (univocamente identificados) indispensáveis à inicialização e operação da EC.

5.2.1.2 Grupo de Trabalho da Política

É responsável por propor todas as políticas da EC, assegurando que se encontram actualizadas. Este grupo deve ter um mínimo de 3 (três) membros.

As responsabilidades deste grupo incluem:

- Definir todas as políticas da EC e garantir que se encontram actualizadas e adaptadas à realidade desta;
- Assegurar que as PC da EC são suportadas pela DPC da EC.
- Assegurar que todos os documentos relevantes e relacionados, directa ou indirectamente, com o funcionamento da EC se encontram armazenados no Ambiente de Informação;
- Assumir o papel de *Administrador de Segurança*, conforme definido no artigo 29º do Decreto Regulamentar n.º 25/2004.

[4] BIOS, conta de administrador do SO, etc

5.2.1.3 Grupo de Trabalho de Operação

É responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC. Note-se que, no sentido de assegurar a disseminação de conhecimento aprofundado sobre a operação da EC, este grupo subdivide-se em 2 (dois) subgrupos, compostos por pelo menos 4 (quatro) membros cada, que deverão revezar-se na participação nas cerimónias da EC. Cada membro apenas pode pertencer exclusivamente a um único subgrupo.

As responsabilidades deste grupo são:

- Gerir o Ambiente de Produção e o Ambiente de 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 correcção das mesmas;
- Pedir a aprovação dos formulários resultantes das cerimónias ao Grupo de Gestão para armazenamento no ambiente de informação.
- Assumir o papel de Administrador de Registo, conforme definido no artigo 29º do *Decreto Regulamentar n.º 25/2004*;
- Assumir o papel de Administrador do Sistema, conforme definido no artigo 29º do *Decreto Regulamentar n.º 25/2004*;
- Assumir o papel de Operador de Sistema, conforme definido no artigo 29º do *Decreto Regulamentar n.º25/2004*.

5.2.1.4 Grupo de Trabalho de Autenticação

É responsável por assegurar a gestão, guarda e disponibilidade (nas situações previstas) das palavras-passe (não pessoais) e dos *tokens* de autorização. Note-se que, no sentido de assegurar altos níveis de segurança e de continuidade de negócio, este grupo subdivide-se em 2 (dois) subgrupos, compostos por pelo menos 3 (três) membros cada, que deverão revezar-se na participação nas cerimónias da EC. Cada membro apenas pode pertencer exclusivamente a um único subgrupo.

Nenhum membro deste grupo está autorizado a entrar no "Ambiente de Operação" sem a presença de um membro do "Grupo de Trabalho de Operação" e/ou do "Grupo de Trabalho de Auditoria".

As responsabilidades deste grupo são:

- Gerir o Ambiente de Autenticação;
- Gerir todas as palavras-passe não pessoais;
- Manter um inventário actualizado de todos os *tokens* de autenticação usados no Ambiente de Produção e, quando os *tokens* estão à responsabilidade de algum(ns) membro(s), registar a identificação desse(s) membro(s), guardando esses registos no Ambiente de Autenticação;
- Manter um inventário actualizado de todas as palavras-passe[5] usadas no Ambiente de Produção e, quando as palavras-passe estão à responsabilidade de algum(ns) membro(s), registar a identificação desse(s) membro(s), guardando esses 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;

[5] Registando o seu valor

- 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 activas de modo a não comprometer cada Ambiente de Produção derivado da perca de um *token*, ou do comprometimento de alguma palavra-passe de autenticação;
- Avaliar pedidos de replicação de documentação.

5.2.1.5 Grupo de Trabalho de Auditoria

É responsável por efectuar a auditoria interna de todas as acções relevantes e necessárias para assegurar a operacionalidade da EC. Este grupo deve ter um mínimo de 1 (um) membro.

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exactidão 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 acções por si realizadas;
- Assumir o papel de Auditor de Sistema, conforme definido no artigo 29º do *Decreto Regulamentar n.º 25/2004*;
- Validar que todos os recursos usados são seguros;
- Verificar periodicamente a integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respectivos[6] e que estão devidamente identificados;
- Verificar periodicamente os registos/logs da EC;
- Gerir o Ambiente de Auditoria.

5.2.1.6 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 vários 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. Este grupo deve ter um mínimo de 2 (dois) membros.

As responsabilidades deste grupo são:

- Gerir o Ambiente de Custódia;

[6] Caso algum deles se encontre requisitado, o Grupo de Trabalho de Auditoria deverá verificar se existe registo do seu levantamento e contactar os elementos envolvidos no sentido de confirmar que o têm em seu poder

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

- Custódia de artefactos sensíveis (*tokens* de autenticação, etc) usando os meios adequados que respondam às necessidades de segurança respectivas;
- Disponibilização segura dos artefactos à sua guarda a membros dos outros grupos e explicitamente autorizados a aceder aos mesmos, após o cumprimento dos procedimentos de identificação e segurança apropriados.

5.2.1.7 Grupo de Trabalho de Gestão

É o órgão decisor da EC da MULTICERT, sendo os seus elementos nomeados e/ou destituídos directamente pelo Conselho de Administração da MULTICERT.

A missão do Grupo de Trabalho de Gestão assenta principalmente na tomada de decisões importantes e criticas ao bom funcionamento da EC MULTICERT, realçando-se a revisão e aprovação de todos os documentos e políticas da EC. O Grupo de Gestão tem ainda como missão a nomeação e/ou destituição dos membros dos restantes grupos e a guarda de alguns artefactos sensíveis (*tokens* de autenticação, etc). Este grupo deve ter um mínimo de 4 (quatro) membros.

As responsabilidades deste grupo são:

- Gerir o Ambiente de Gestão;
- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Políticas;
- Divulgar novas políticas aos restantes membros dos Grupos;
- Designar os membros dos restantes grupos de trabalho???
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários grupos de trabalho, em um ou mais locais facilmente acessíveis pelos indivíduos autorizados;
- Tomar decisões críticas sobre o funcionamento da EC;
- Rever e aprovar todos os formulários resultantes das cerimónias executadas e todos os documentos relacionados com o funcionamento da EC.

5.2.2 Número de pessoas exigidas por tarefa

Existem rigorosos procedimentos de controlo que obrigam à divisão de responsabilidades baseada nas especificidades da 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 recepção e inspecção até à destruição física e/ou lógica do hardware. Após a activação 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 activação e vice-versa.

5.2.3 Funções que requerem separação de responsabilidades

A matriz seguinte define as incompatibilidades (assinaladas por ✖) entre a pertença ao grupo/subgrupo identificado nas colunas e a pertença ao grupo/subgrupo identificado nas linhas, no contexto desta EC:

Se pertence ao Grupo/Subgrupo ...	Pode pertencer ao Grupo/Subgrupo ...?	Instalação	Políticas	Operação		Autenticação		Auditoria	Custódia	Gestão
				Subgrupo 1	Subgrupo 2	Subgrupo 1	Subgrupo 2			
Instalação								×	×	×
Políticas								×	×	×
Operação	**Subgrupo 1**				×	×	×	×	×	×
	Subgrupo 2			×		×	×	×	×	×
Autenticação	**Subgrupo 1**			×	×		×	×	×	×
	Subgrupo 2			×	×	×		×	×	×
Auditoria		×	×	×	×	×	×		×	×
Custódia		×	×	×	×	×	×	×		×
Gestão		×	×	×	×	×	×	×	×	

5.3 Medidas de Segurança de Pessoal

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

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

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

A admissão de novos membros nos Grupos de Trabalho é apenas possível se apresentarem provas de conhecimento, qualificações e experiência necessárias para a realização das tarefas dos Grupos de Trabalho, assim como devem ter credenciações governamentais, no mínimo equivalentes a NACIONAL SECRETO.

5.3.2 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[8] inclui:

- confirmação de identificação, usando documentação emitida por fontes fiáveis, e
- investigação de registos criminais.

5.3.3 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 Infra-estruturas de Chave Publica;
b) conceitos gerais sobre segurança da informação;
c) formação especifica para o seu papel dentro do Grupo de Trabalho;
d) funcionamento do software e/ou hardware usado pela EC;
e) politica de Certificados e Declaração de Práticas de Certificação;
f) recuperação face a desastres;
g) procedimentos para a continuidade da actividade e
h) aspectos legais básicos relativos à prestação de serviços de certificação.

5.3.4 Frequência e requisitos para acções 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 existe qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afecto às EC,
- sempre que são introduzidas alterações nas Politicas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos das EC.

5.3.5 Frequência e sequência da rotação de funções

Nada a assinalar.

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

5.3.6 Sanções para acções não autorizadas

Consideram-se acções não autorizadas todas as acções 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 de trabalho, legislação nacional e das leis de segurança nacional, a todos os indivíduos que realizem acções não autorizadas ou que façam uso não autorizado dos sistemas.

5.3.7 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 directamente supervisionados pelos membros do Grupo de Trabalho.

Os procedimentos de verificação de antecedentes a aplicar nestas situações são os mesmos que são indicados na secção 5.3.2.

5.3.8 Documentação fornecida ao pessoal

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

5.4 Procedimentos de auditoria de segurança

5.4.1 Tipo de eventos registados

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

- pedido, emissão, renovação, re-emissão e revogação de certificados;
- publicação de LRC;
- eventos relacionados com segurança, incluindo:
    - tentativas de acesso (com e sem sucesso) a recursos sensíveis da EC;
    - operações realizadas por membros dos Grupos de Trabalho,
    - dispositivos físicos de segurança de entrada / saída dos vários níveis de segurança.

As entradas nos registos incluem a informação seguinte:

- número de série do evento;
- data e hora do evento;
- identidade do sujeito que causou o evento;
- categoria do evento;
- descrição do evento.

5.4.2 Frequência da auditoria de registos

Os registos são analisados e revistos de modo regular, e adicionalmente sempre que haja suspeitas ou actividades anormais ou ameaças de algum tipo. Acções tomadas baseadas na informação dos registos são também documentadas.

5.4.3 Período de retenção dos registos de auditoria

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

5.4.4 Protecção dos registos de auditoria

Os registos são apenas analisados por membros autorizados dos Grupos de Trabalho.

Os registos são protegidos por mecanismos electrónicos auditáveis de modo a detectar e impedir a ocorrência de tentativas de modificação, remoção ou outros esquemas de manipulação não autorizada dos dados.

5.4.5 Procedimentos para a cópia de segurança dos registos

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

5.4.6 Sistema de recolha de registos (Interno / Externo)

Os registos são recolhidos em simultâneo interna e externamente ao sistema da EC.

5.4.7 Notificação de agentes causadores de eventos

Eventos auditáveis são registados no sistema de auditoria e guardados de modo seguro, sem haver notificação ao sujeito causador da ocorrência do evento.

5.4.8 Avaliação de vulnerabilidades

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

5.5 Arquivo de registos

5.5.1 Tipo de dados arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

5.5.2 Período de retenção em arquivo

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

5.5.3 Protecção dos arquivos

O arquivo é protegido de modo a que:

- apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo,
- o arquivo é protegido contra qualquer modificação ou tentativa de o remover,

- o arquivo é protegido contra a deterioração do media onde é guardado, através de migração periódica para media novo,
- o arquivo é protegido contra a obsolescência do hardware, sistemas operativos e outros software, pela conservação do hardware, sistemas operativos e outros software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal e
- os arquivos são guardados de modo seguro em ambientes externos seguros.

5.5.4 Procedimentos para as cópias de segurança do arquivo

Cópias de segurança dos arquivos são efectuados de modo incremental ou total e guardados em dispositivos apropriados.

5.5.5 Requisitos para validação cronológica dos registos

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

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

Os sistemas de recolha de dados de arquivo são internos.

5.5.7 Procedimentos de recuperação e verificação de informação arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos. A integridade do arquivo deve ser verificada através da sua restauração.

5.6 Renovação de chaves

Nada a assinalar.

5.7 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.

5.7.1 Procedimentos em caso de incidente ou comprometimento

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

5.7.2 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 re-estabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a EC MULTICERT suspenderá os seus serviços e notificará a Autoridade Credenciadora.

5.7.3 Procedimentos em caso de comprometimento da chave privada da entidade

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

- revogação do certificado da EC MULTICERT e de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC MULTICERT,
- notificação da Autoridade Credenciadora e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC MULTICERT,
- geração de novo par de chaves para a EC MULTICERT,
- renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC MULTICERT.

5.7.4 Capacidade de continuidade da actividade em caso de desastre

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

5.8 Procedimentos em caso de extinção de EC ou ER

Em caso de cessação de actividade como prestador de serviços de Certificação, a EC MULTICERT deve, atempadamente, com uma antecedência mínima de três meses, proceder às seguintes acções:

a) informar a Autoridade Credenciadora;

b) informar todos os titulares de certificados;

c) revogar todos os certificados emitidos;

d) efectuar uma notificação final aos titulares 2 (dois) dias antes da cessação formal da actividade;

e) garantir a transferência (para retenção por outra organização) de toda a informação relativa à actividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

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

6 MEDIDAS DE SEGURANÇA TÉCNICAS

Esta secção define as medidas de segurança implementadas para a EC MULTICERT de forma a proteger chaves criptográficas geradas por esta, e respectivos dados de activação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras assim como dados de activação estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

6.1 Geração e instalação do par de chaves

A geração dos pares de chaves da EC MULTICERT são processados de acordo com os requisitos e algoritmos definidos nesta politica.

6.1.1 Geração do par de chaves

A geração de chaves criptográficas da EC MULTICERT auto-assinada 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 EC MULTICERT, cumpre os requisitos FIPS 140-1 nível 3 e/ou *Common Criteria EAL* 4+ e, efectua 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 politicas 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 efectuadas 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 chave privada para os certificados de pessoa singular e de pessoa colectiva são gerados pela EC MULTICERT, usando hardware criptográfico que cumpre os requisitos FIPS 140-1 nível 3 e/ou *Common Criteria EAL* 4+.

O funcionamento da EC MULTICERT é efectuado em modo *on-line*.

6.1.2 Entrega da chave privada ao titular

A entrega da chave privada associada aos certificados de pessoa singular e de pessoa colectiva é efectuada em dispositivo criptográfico SSCD (*Secure Signature-Creation Device*).

6.1.3 Entrega da chave pública ao emissor do certificado

A chave pública é entregue à EC MULTICERT, de acordo com os procedimentos indicados na secção 4.3.1.

6.1.4 Entrega da chave pública da EC às partes confiantes

A chave pública da EC MULTICERT será disponibilizada através do certificado da EC MULTICERT, conforme secção 2.2.

6.1.5 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 EC MULTICERT,
- 2048 bits RSA para as chaves associadas aos certificados de equipamento tecnológico,
- 2048 bits RSA para as chaves associadas aos certificados de pessoa singular e de pessoa colectiva.

6.1.6 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.

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

De acordo com secção 7.1.

6.2 Protecção da chave privada e características do módulo criptográfico

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

6.2.1 Normas e medidas de segurança do módulo criptográfico

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

- Segurança Física
  - *Common Criteria EAL* 4+ e/ou
  - FIPS 140-1, nível 3
- Certificações Regulamentares
  - U/L 1950 & CSA C22.2 safety compliant
  - FCC Part 15 – Class B
  - Certificação ISO – 9002
- Papéis
  - autenticação de dois factores
- Suporte de API
  - PKCS#11

- Microsoft CryptoAPI
- Java JCE/JCE CSP
- Open SSL

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

– Troca de chaves e chave de cifra assimétrica
  - RSA (512-4096 bit), PKCS#1 v1.5, OAEP PKCS#1 v2.0
  - Diffie-Hellman (512-1024 bit)

– Assinatura Digital
  - RSA (512-4096 bit)
  - DSA (512-1024 bit)
  - PKCS#1 v1.5

– Algoritmos de chave simétrica
  - DES
  - 3DES (comprimento duplo e triplo)
  - RC2
  - RC4
  - RC5
  - AST
  - CAST-3
  - CAST-128

– Algoritmos de Hash
  - SHA-1
  - MD-2
  - MD-5

– Códigos de Autenticação de Mensagens (*Message Authentication Codes* - MAC)
  - HMAC-MD5
  - HMAC-SHA-1
  - SSL3-MD5-MAC
  - SSL3-SHA-1-MAC

6.2.2 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 MULTICERT implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efectuar operações criptográficas sensíveis na EC.

Os dados de activação necessários para a utilização da chave privada da EC MULTICERT são divididos em várias partes (guardadas nas chaves PED – pequenos tokens de identificação digital, com o formato de caneta USB, 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 numero de partes (m) é necessário para activar a chave privada da EC MULTICERT guardada no módulo

criptográfico em hardware. São necessárias duas (n) partes para a activação da chave privada da EC MULTICERT.

6.2.3 Retenção da chave privada (key escrow)

A retenção da chave privada da EC MULTICERT é explicada em detalhe na secção 4.12.

6.2.4 Cópia de segurança da chave privada

A chave privada da EC MULTICERT tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original, conforme secção 4.12.

6.2.5 Arquivo da chave privada

As chaves privadas da EC MULTICERT, alvo de cópias de segurança, são arquivadas conforme identificado na secção 4.12.

6.2.6 Transferência da chave privada para/do módulo criptográfico

As chaves privadas da EC MULTICERT não são exportáveis a partir do *token* criptográfico FIPS 140-1 nível 3.

Mesmo se for feito uma cópia de segurança das chaves privadas da EC MULTICERT para um outro *token* criptográfico, essa cópia é feita directamente, hardware para hardware, de uma forma que garante o transporte das chaves entre módulos numa transmissão cifrada.

6.2.7 Armazenamento da chave privada no módulo criptográfico

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

6.2.8 Processo para activação da chave privada

A EC MULTICERT é uma EC *on-line*, cuja chave privada é activada quando o sistema da EC é ligado. Esta activação é efectivada através da autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação de dois factores (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 (membros dos grupos de trabalho), cada uma delas possuindo uma chave PED, são obrigadas a autenticar-se antes que seja possível efectuar a cópia de segurança.

Para a activação das chaves privadas da EC MULTICERT é necessária, no mínimo, a intervenção de quatro elementos do Grupo de Trabalho. Uma vez a chave activada, esta permanecerá assim até que o processo de desactivação seja executado.

6.2.9 Processo para desactivação da chave privada

A chave privada da EC MULTICERT é desactivada quando o sistema da EC é desligado.

Para a desactivação das chaves privadas da EC MULTICERT é necessária, no mínimo, a intervenção de quatro elementos do Grupo de Trabalho. Uma vez desactivada, esta permanecerá inactiva até que o processo de activação seja executado.

6.2.10 Processo para destruição da chave privada

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

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

6.2.11 Avaliação/nível do módulo criptográfico

Descrito na secção 6.2.1.

6.3 Outros aspectos da gestão do par de chaves

6.3.1 Arquivo da chave pública

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

6.3.2 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 EC MULTICERT tem uma validade mínima de onze anos e quatro meses, sendo utilizado para assinar certificados durante os seus primeiros cinco anos de validade, sendo reemitido após os primeiros quatro anos e nove meses de validade;
- os certificados de equipamento tecnológico (à excepção do certificado de servidor Web) têm uma validade máxima de cinco anos e dois meses, sendo utilizados durante o seu primeiro mês de validade, sendo reemitido após o primeiro mês de validade;
- o certificado de servidor Web tem uma validade máxima de cinco anos e um mês, sendo reemitido um mês antes do final da sua validade;
- o certificado de pessoa singular tem uma validade máxima de cinco anos;
- o certificado de pessoa colectiva tem uma validade máxima de cinco anos.

6.4 Dados de activação

6.4.1 Geração e instalação dos dados de activação

Os dados de activação necessários para a utilização da chave privada da EC MULTICERT são divididos em várias partes (guardadas em chaves PED – pequenos *tokens* de identificação digital, com o formato de caneta USB – 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 140-1 nível 3.

6.4.2 Protecção dos dados de activação

Os dados de activação (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 EC MULTICERT são guardadas, de forma cifrada, em *token* criptográfico.

6.4.3 Outros aspectos dos dados de activação

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

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

6.5 Medidas de segurança informáticas

6.5.1 Requisitos técnicos específicos

O acesso aos servidores da EC MULTICERT é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. A EC MULTICERT tem um funcionamento on-line, sendo o pedido de emissão de certificados efectuado a partir do Sistema de Gestão do Ciclo de Vida dos Certificados (SGCVC) e/ou da consola de operação.

A EC MULTICERT e o SGCVC dispõem de dispositivos de protecção de fronteira, nomeadamente sistema firewall, assim como cumprem os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.5.2 Avaliação/nível de segurança

Os vários sistemas e produtos empregue pela EC MULTICERT são fiáveis e protegidos contra modificações.

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

6.6 Ciclo de vida das medidas técnicas de segurança

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

6.6.2 Medidas para a gestão da segurança

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

6.6.3 Ciclo de vida das medidas de segurança

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

6.7 Medidas de Segurança da rede

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

6.8 Validação cronológica (Time-stamping)

Certificados, CRLs e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. Tal informação não é baseada em mecanismos criptográficos.

7 PERFIS DE CERTIFICADO, CRL, E OCSP

7.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correcto (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 efectuado 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.[3]

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar 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. [3]

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

- Recomendação ITU.T X.509[9],
- RFC 5280[3], e
- Legislação nacional e Europeia aplicável.

Os perfis dos certificados podem ser consultadas nos documentos de Políticas de Certificados associadas a esta DPC, de acordo com tabela da secção 3.1.1.

7.2 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.[3]

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC). 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

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

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.[3]

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[9],
- RFC 5280[3], e
- Legislação nacional e Europeia aplicável.

Os perfis das LRC podem ser consultadas nos documentos de Políticas de Certificados associadas a esta DPC, relativamente à EC MULTICERT (de acordo com tabela da secção 3.1.1).

7.3 Perfil OCSP

O perfil dos certificados OCSP está de acordo com:

- Recomendação ITU.T X.509[9],
- RFC 5280[3], e
- Legislação nacional e Europeia aplicável.

Os perfis dos certificados OCSP podem ser consultadas no documento de Política de Certificados de Validação on-line OCSP associadas a esta DPC, de acordo com tabela da secção 3.1.1.

8 AUDITORIA E AVALIAÇÕES DE CONFORMIDADE

Uma inspecção 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 EC MULTICERT.

Para além de auditorias de conformidade, a MULTICERT irá efectuar outras fiscalizações e investigações para assegurar a conformidade da EC MULTICERT com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

8.1 Frequência ou motivo da auditoria

As auditorias de conformidade são realizadas regularmente de acordo com a legislação[10]. A EC precisa de provar, com a auditoria e relatório de segurança anuais (produzidos pelo auditor de segurança acreditado), que a avaliação dos riscos foi assegurada, tendo sido identificado e implementado todas as medidas necessárias para a segurança de informação.

8.2 Identidade e qualificações do auditor

O auditor é uma figura independente do círculo de influência da Entidade de Certificação, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infra-estruturas de chaves pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança. A sua missão é auditar a infra-estrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, em Março, à Autoridade Credenciadora.

A Autoridade Credenciadora é responsável pela credenciação do Auditor de Segurança, de acordo com os requisitos e qualificações identificados em http://www.gns.gov.pt/gns/pt/assinatura/[11]. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Autoridade Credenciadora podem ser encontrados em http://www.gns.gov.pt/gns/pt/assinatura/ .

A EC MULTICERT promove uma política de rotação dos seus auditores de seguranças, tal como as melhores práticas prevêem. Os auditores de segurança da EC MULTICERT foram/são os seguintes:

NOME	Data início – Data de fim
Paulo Jorge Martins Borges	15/Dez/2008 –

8.3 Relação entre o auditor e a Entidade Certificadora

O auditor e membros da sua equipa são independentes, não actuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

[10] cf. Decreto Regulamentar n.º 25/2004, de 15 de Julho.
[11] Norma Técnica – D 01, Requisitos para a Credenciação de Auditor de Segurança previstos no Decreto Regulamentar nº 25/2004, de 15 de Julho, Gabinete Nacional de Segurança, 2007

Na Relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual.

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

O cumprimento do estabelecido na legislação em vigor sobre a protecção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares das EC.

8.4 Âmbito da auditoria

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

8.5 Procedimentos após uma auditoria com resultado deficiente

Se duma auditoria resultarem irregularidades, o auditor procede da seguinte forma:

a) documenta todas as deficiências encontradas durante a auditoria;

b) no final da auditoria reúne com os responsáveis da entidade submetida a auditoria e apresenta de forma resumida um relatório de primeiras impressões (RPI);

c) elabora o relatório de auditoria. Este relatório deverá estar organizado de modo a que todas as deficiências sejam escalonadas por ordem decrescente de gravidade/severidade;

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

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

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

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

   a. aceitam os termos, permitindo que a actividade seja desenvolvida até à próxima inspecção;

   b. permitem que a entidade continue em actividade por um período máximo de 60 dias até à correcção das irregularidades antes da revogação;

   c. revogação imediata da actividade.

8.6 Comunicação de resultados

Os resultados devem ser comunicados de acordos com os prazos estabelecidos no quadro seguinte:

COMUNICAÇÃO DE RESULTADOS	AUDITOR	ENTIDADE	ENTIDADE
RPI	No final da auditoria		
RAF	2 semanas		

RCI		1 semana	
Decisão sobre irregularidades			1 semana

9 OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

Esta secção aborda aspectos de negócio e assuntos legais.

9.1 Taxas

9.1.1 Taxas por emissão ou renovação de certificados

A serem identificadas em proposta formal a efectuar pela MULTICERT.

9.1.2 Taxas para acesso a certificado

Nada a assinalar.

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

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

9.1.4 Taxas para outros serviços

As taxas para os serviços de validação cronológica e validação on-line OCSP são identificadas em proposta formal a efectuar pela MULTICERT.

9.1.5 Política de reembolso

Nada a assinalar.

9.2 Responsabilidade financeira

9.2.1 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.

9.2.2 Outros recursos

Nada a assinalar.

9.2.3 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.

9.3 Confidencialidade da informação processada

9.3.1 Âmbito da confidencialidade da informação

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

a) as chaves privadas da EC MULTICERT;

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

c) toda a informação de carácter pessoal proporcionada à EC 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 transacções, incluindo os registos completos e os registos de auditoria das transacções;

f) informação de todos os documentos relacionados com a EC 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 EC 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, PINs e outros elementos de segurança relacionados com a EC MULTICERT;

h) a identificação dos membros dos grupos de trabalho da EC MULTICERT;

i) a localização dos ambientes da EC MULTICERT e seus conteúdos.

9.3.2 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,

d) Delta-LRC e

e) toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

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

9.3.3 Responsabilidade de protecção da confidencialidade da informação

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

9.4 Privacidade dos dados pessoais

9.4.1 Medidas para garantia da privacidade

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

9.4.2 Informação privada

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

9.4.3 Informação não protegida pela privacidade

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

9.4.4 Responsabilidade de protecção da informação privada

De acordo com a legislação portuguesa.

9.4.5 Notificação e consentimento para utilização de informação privada

De acordo com a legislação portuguesa.

9.4.6 Divulgação resultante de processo judicial ou administrativo

Nada a assinalar.

9.4.7 Outras circunstâncias para revelação de informação

Nada a assinalar.

9.5 Direitos de propriedade intelectual

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

9.6 Representações e garantias

9.6.1 Representação e garantias das entidades certificadoras

A EC 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 "Suspensão e Revogação de Certificados" deste documento e publicar os certificados revogados na LRC do repositório da EC MULTICERT, com a frequência estipulada na secção 4.9.7.,

m) publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões actuais assim como as versões anteriores,

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

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 4.9.7,

s) em caso de cessar a sua actividade 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 Protecção 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 EC MULTICERT.

9.6.2 Representação e garantias das Entidades de Registo

Nada a assinalar.

9.6.3 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 4.9.3,

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 exacta 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 efectuar acções de "engenharia inversa" sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da EC MULTICERT.

9.6.4 Representação e garantias das partes confiantes

É obrigação das partes que confiem nos certificados emitidos pela EC 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 correcta 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,

f) notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando os meios que a EC MULTICERT publique no seu sítio Web.

9.6.5 Representação e garantias de outros participantes

Nada a assinalar.

9.7 Renúncia de garantias

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

9.8 Limitações às obrigações

a) a EC MULTICERT responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua actividade de acordo com o Artº 26 do DL 62/2003.

b) a EC MULTICERT 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) a EC MULTICERT assume toda a responsabilidade mediante terceiros pela actuação dos titulares das funções necessárias à prestação de serviços de certificação.

d) a responsabilidade da administração / gestão da EC MULTICERT assenta sobre base objectivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços

e) a EC MULTICERT 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) a EC MULTICERT 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) a EC MULTICERT não responde se o destinatário dos documentos assinados electronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações e

h) a EC MULTICERT não assume qualquer responsabilidade no caso de perca ou prejuízo:

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

   iii) ocasionados pelo uso dos 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 EC MULTICERT.

9.9 Indemnizações

De acordo com a legislação em vigor

9.10 Termo e cessação da actividade

9.10.1 Termo

Os documentos relacionados com a EC MULTICERT (incluindo esta DPC) tornam-se efectivos 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 EC MULTICERT.

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

9.10.2 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 EC 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 efectuadas 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.

9.10.3 Consequências da cessação de actividade

Após o Grupo de Trabalho de Gestão decidir em favor da eliminação de um documento relacionado com a EC, o Grupo de Trabalho das Políticas 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 EC MULTICERT, nascidas sob sua vigência, subsistirão após sua substituição ou revogação por uma nova versão em tudo o que não se oponha a esta.

9.11 Notificação individual e comunicação aos participantes

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

9.12 Alterações

9.12.1 Procedimento para alterações

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

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

O Grupo de Trabalho da Política vai rever o pedido feito e, se verificar a sua pertinência, procede às actualizações 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 afectadas (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 da Política 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 efectivas.

9.12.2 Prazo e mecanismo de notificação

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

9.12.3 Motivos para mudar de OID

O Grupo de Trabalho da Política 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 da Política, as alterações da DPC não afectem à aceitação dos certificados proceder-se-á ao aumento do número menor de versão do documento e o último número de Identificador de Objecto (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 da Política julgue que as alterações à especificação podem afectar 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 Objecto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 9.12.2.

9.13 Disposições para resolução de conflitos

Todas reclamações entre utilizadores e EC 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

9.14 Legislação aplicável

É aplicável à actividade 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.

9.15 Conformidade com a legislação em vigor

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

É responsabilidade da Autoridade Credenciadora zelar pelo cumprimento da legislação aplicável listada na secção 9.14.

9.16 Providências várias

9.16.1 Acordo completo

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

9.16.2 Independência

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

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

9.16.3 Severidade

Nada a assinalar.

9.16.4 Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

9.16.5 Força Maior

Nada a assinalar.

9.17 Outras providências

Nada a assinalar.

Conclusão

Este documento define os procedimentos e práticas utilizadas pela Entidade de Certificação MULTICERT no suporte à sua actividade de certificação digital. A hierarquia de confiança da Entidade de Certificação MULTICERT:

- fornece uma hierarquia de confiança, que promoverá a segurança electrónica do titular dos certificados no seu relacionamento com terceiras partes,
- proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

Referências Bibliográficas

Decreto-Lei n.º 290-D/99, de 2 de Agosto.

Decreto-Lei n.º 62/2003, de 3 de Abril.

Decreto Regulamentar n.º 25/2004, de 15 de Julho.

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

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

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

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

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

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

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

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

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

RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

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

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

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

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

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

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