multicert
Engineering for digital security

Declaração de Práticas de Certificação da MULTICERT Trust Services Certification Authority

Políticas

MULTICERT_PJ.ECRAIZ_127.doc

Identificação do Projeto: ECRAIZ

Identificação da CA: MULTICERT TS CA

Nível de Acesso: Público

Versão: 2.0

Data: 27/03/2016

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

Identificador do documento: MULTICERT_PJ.ECRAIZ_127.doc

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

Tipologia documental: Políticas

Título: Declaração de Práticas de Certificação da MULTICERT Trust Services Certification Authority

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 27/03/2016

Versão atual: 2.0

Identificação do Projeto: ECRAIZ

Identificação da CA: MULTICERT TS CA

Cliente: MULTICERT S.A.

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
0.1	13/02/2014	Versão inicial	MULTICERT
0.2	12/06/2014	Revisão	MULTICERT
1.0	13/06/2014	Versão Aprovada	MULTICERT
1.1-1.5	21/08/2015	Revisão	MULTICERT
2.0	27/03/2016	Versão Aprovada	MULTICERT

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.2_0004_pt.doc	Política de Certificado de Validação Cronológica	MULTICERT
MULTICERT_PJ.CA3_24.1.2_0005_pt.doc	Política de Certificado de Validação on-line OCSP	MULTICERT

Resumo Executivo

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

A infraestrutura da MULTICERT *Trust Services Certification Authority* (MULTICERT TS CA), fornece uma hierarquia de confiança, que promove a segurança eletrónica dos demais serviços terceira parte de confiança. A MULTICERT TS CA, estabelece uma estrutura de confiança eletrónica que proporciona a autenticidade, integridade e não repúdio de serviços de segurança associados a Entidades de Certificação.

A MULTICERT TS CA está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014, conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir certificados digitais para serviços de confiança.

Este documento define os procedimentos e práticas utilizadas pela MULTICERT TS CA no suporte à sua atividade de certificação digital, sendo referenciado como o documento de Declaração de Práticas de Certificação da MULTICERT *Trust Services Certification Authority*.

Sumário

Introdução

Objetivos

O objetivo deste documento é definir os procedimentos e práticas utilizadas pela MULTICERT *Trust Services Certification Authority* (MULTICERT TS CA) no suporte à sua atividade de certificação digital.

Público-Alvo

Este documento deve ser lido por:

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

Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. 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 MULTICERT TS CA. 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 objetivo 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, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve as práticas gerais de emissão e gestão de certificados, seguidas pela MULTICERT *Trust Services Certification Authority* (MULTICERT TS CA) 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 MULTICERT TS CA. Este documento pode sofrer atualizações regulares.

Os certificados emitidos pela MULTICERT TS CA contêm uma referência à 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 MULTICERT TS CA 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 infraestrutura de Chaves Públicas ("*PKI – Public Key Infrastructure*").

Esta DPC aplica-se especificamente à MULTICERT TS CA que 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*;
- ETSI TS 102 042; *Policy requirements for certification authorities issuing public key certificates, v2.4.1*.

1.2 Designação e Identificação do Documento

Este documento é a Declaração de Práticas de Certificação da MULTICERT TS CA. A DPC é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento o 1.3.6.1.4.1.25070.1.1.1.2.0.7

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 2.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.2.0.7
Data de Emissão	27/03/2016
Validade	1 Ano
Localização	https://pki.multicert.com/index.html

1.3 Participantes na Infraestrutura de Chave Pública

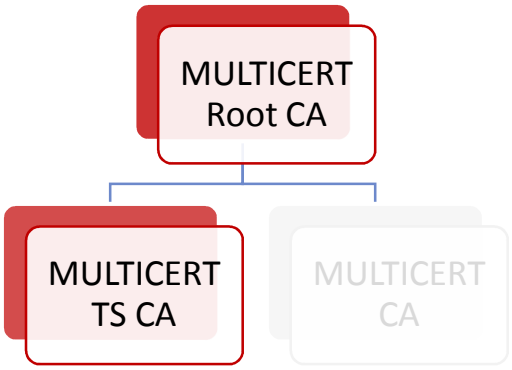
Entidades Certificadoras

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

- Hierarquia de confiança auto-assinada própria, para efeitos de independência em relação a outras hierarquias de confiança;
- Hierarquia MULTICERT, assinada pela MULTICERT Root CA.

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

Esquematicamente:



INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	CN=MULTICERT *Trust Services Certification Authority* 001, OU = Entidade de Certificação Credenciada, O = MULTICERT - Serviços de Certificação Electrónica S.A.,C = PT

Entidades de Registo

Não existem entidades de registo. Os serviços internos da MULTICERT TS CA procedem ao registo e validação dos dados necessários para a emissão de certificados.

Titulares de certificados

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

São considerados titulares de certificados emitidos pela MULTICERT TS CA, aqueles cujo nome está inscrito no campo "Assunto" (*Subject)* do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificados, descritas neste documento.

A MULTICERT TS CA emite certificados para:

- *Object Signing;*
- *Code Signing* (Assinatura de código);
- Serviço de Validação Cronológica;
- Serviço de Listas de Estado de Confiança (TSL), e
- Serviço de Validação *on-line* OCSP.

Partes Confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou serviços 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 MULTICERT TS CA.

Outros participantes

Autoridade Credenciadora

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

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

A Autoridade Credenciadora é uma das "peças" que contribui para a confiabilidade dos Certificados emitidos, pelas competências que exerce sobre as EC que os emitem. No âmbito das suas funções, a Autoridade Credenciadora, exerce os seguintes papéis relativamente às ECs:

a) **Credenciação**: procedimento de aprovação da EC para exercer a sua atividade, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, o 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 inspeções efetuadas às EC, com vista a regularmente verificar parâmetros de conformidade;
d) **Auditor de Segurança**: figura independente do círculo de influência da EC e que lhe é exigida.

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 atual 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 MULTICERT TS CA.

Entidade de Validação Cronológica

As Entidades de Validação cronológica emitem selos temporais eletrónicos, que atestam a data e hora da criação, expedição ou receção de um documento eletrónico.

O serviço de Entidade de Validação Cronológica é disponibilizado pela MULTICERT TS CA.

Auditor de Segurança

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

A MULTICERT TS CA promove uma política de rotação dos seus auditores de seguranças, tal como as melhores práticas preveem.

1.4 Utilização do Certificado

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

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

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a MULTICERT TS CA 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.

Utilização adequada

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

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

Os certificados emitidos para efeitos de utilização por serviços de confidencialidade, emitidos com base nas regras aqui definidas, podem ser utilizados para processar informação classificada até o grau de CONFIDENCIAL quando utilizados sobre redes públicas (p.e. Internet). Na sua utilização em redes

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

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 MULTICERT TS CA são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob a MULTICERT TS CA, 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 MULTICERT TS CA.

Utilização não autorizada

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

Os certificados emitidos pela MULTICERT TS CA não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela MULTICERT TS CA, não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram um atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

1.5 Gestão das Políticas

Entidade responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do Grupo de Trabalho de Autenticação da MULTICERT TS CA.

Contato

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

Entidade responsável pela determinação da conformidade da DPC relativamente à Política

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

Procedimentos para Aprovação da DPC

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

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

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

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

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

- Disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização, garantindo-se durante o tempo da disponibilidade:
    - Mínimo de 99,990% de respostas a pedidos de obtenção da LRC;
    - Mínimo de 99,990% de respostas a pedidos do documento da DPC;
- Número máximo de pedidos de LRC: 50 pedidos/minuto;
- Número máximo de pedidos da DPC: 50 pedidos/minuto;
- Número médio de pedidos de LRC: 20 pedidos/minuto;
- Número médio de pedidos da DPC: 20 pedidos/minuto.

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

- 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 atuais de segurança física e lógica,
- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

2.2 Publicação de informação de certificação

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

A MULTICERT S.A. disponibiliza sempre a seguinte informação pública *on-line*:

- Cópia eletrónica deste DPC e Políticas de Certificados (PC) mais atuais da MULTICERT TS CA, assinada eletronicamente, por individuo devidamente autorizado e com certificado digital atribuído para o efeito:
    - DPC da MULTICERT TS CA disponibilizada no URI: https://pki.multicert.com/index.html,
    - PC de certificado auto-assinado da MULTICERT TS CA disponibilizada no URI: https://pki.multicert.com/index.html,
    - PC de certificado de Validação *on-line* OCSP disponibilizada no URI: https://pki.multicert.com/index.html,
    - PC de certificado de Validação Cronológica disponibilizada no URI: https://pki.multicert.com/index.html,
- LRC da MULTICERT TS CA – URI: https://pki.multicert.com/index.html;

- Delta-LRC da MULTICERT TS CA – URI: https://pki.multicert.com/index.html;
- Certificado da MULTICERT TS CA – URI: https://pki.multicert.com/index.html;
- Outra informação relevante – URI: https://pki.multicert.com/index.html

Adicionalmente, serão conservadas todas as versões anteriores das PCs e DPCs da MULTICERT TS CA, 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 atualizações a esta DPC e respetivas PCs serão publicadas imediatamente após a sua aprovação pelo Grupo de Gestão, de acordo com a secção 0.

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

2.4 Controlo de acesso aos repositórios

A informação publicada pela MULTICERT TS CA, está disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso somente para leitura). A MULTICERT TS CA 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:

- Ao certificado de é atribuído o nome qualificado do domínio e/ou o âmbito da sua utilização.

Tipos de nomes

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

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

Tipo de Certificado	OID da Política de Certificados
MULTICERT TS CA (auto-assinada)	1.3.6.1.4.1.25070.1.1.1.2.0.1.5
Validação *on-line* OCSP	1.3.6.1.4.1.25070.1.1.1.0.1.3
Validação Cronológica	1.3.6.1.4.1.25070.1.1.1.2.0.1.1
Code Signing	1.3.6.1.4.1.25070.1.1.1.2.0.1.2
TSL	1.3.6.1.4.1.25070.1.1.1.2.0.1.3
Object Signing	1.3.6.1.4.1.25070.1.1.1.2.0.1.4

Necessidade de nomes significativos

A MULTICERT TS CA irá assegurar dentro da sua hierarquia de confiança, a não existência de certificados que, tendo o mesmo nome único, identifiquem entidades ou serviços distintos.

Anonimato ou pseudónimo de titulares

A MULTICERT TS CA não emite certificados com pseudónimo.

Interpretação de formato de nomes

As regras utilizadas pela MULTICERT TS CA 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 exceção dos atributos *country* e *serialnumber* que são codificados numa *PrintableString*.

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

Unicidade de nomes

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

De acordo com os seus processos de emissão, a MULTICERT TS CA rejeita a emissão de certificados com o mesmo DN para titulares distintos. Para cada tipo de certificado emitido, a respetiva 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.

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 MULTICERT TS CA, infringir os direitos de propriedade intelectual de outros indivíduos ou entidades.

No procedimento de autenticação e identificação dos representantes legais 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 respetiva Política de Certificado descreve todos os passos necessários, desde o início do pedido de certificado até à atribuição do certificado digital aos responsáveis pelo mesmo.

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).

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.

Identificação e autenticação para renovação de chaves, após revogação

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

3.4 Identificação e autenticação para pedido de revogação

O processo de Revogação de certificados emitidos pela MULTICERT TS CA, inicia-se sempre com a SUSPENSÃO, permitindo que a validação do pedido de revogação seja devidamente validado.

Quem pode solicitar a Revogação de um Certificado

O pedido de Revogação poderá ser efetuado por um dos seguintes intervenientes:

- O Titular,
- A Entidade Requerente do certificado,
- A MULTICERT, sempre que esta tenha conhecimento de que os dados constantes no certificado não correspondem à realidade, ou não se encontre em posse do titular.

Após rececionado o pedido de revogação de um certificado, será efetuada a validação da documentação recebida. A identificação e autenticação dos intervenientes no pedido de revogação será efetuado através da verificação, por semelhança, das assinaturas constantes no formulário, com as cópias dos documentos de identificação solicitados.

Como solicitar a Revogação do Certificado

O Pedido de Revogação poderá ser efetuado de duas formas:

- On-line, através do serviço disponibilizado para o efeito, num dos seguintes endereços abaixo listados, sendo que o certificado passará para o estado SUSPENSO e só após rececionada e devidamente validada a documentação inerente ao pedido, a MULTICERT poderá alterar o estado do certificado para REVOGADO:
    - Interface de suspensão de certificados emitidos até 26/05/2015 (certificados com referência MAE ou MRA): https://pki.multicert.com/suspensao;
    - Interface de suspensão de certificados emitidos a partir de 27/05/2015 (certificados com referência MTC): https://www.multicert.com/suspensao.
- Ou, Enviando diretamente para a MULTICERT, o Formulário de Pedido de Revogação, disponibilizado pela MULTICERT, devidamente preenchido e acompanhado da documentação necessária para o efeito.

4 Requisitos operacionais do ciclo de vida do certificado

4.1 Pedido de Certificado

4.2 Para cada tipo de certificados, a respetiva Política de Certificado descreve o pedido de certificado.Processamento do pedido de certificado

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

4.3 Emissão de Certificado

4.4 Para cada tipo de certificados, a respetiva Política de Certificado descreve a emissão de certificado.Aceitação do Certificado

Para cada tipo de certificados, a respetiva 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 respetiva 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 exceção do período de validade do certificado.

Esta prática não é suportada na MULTICERT TS CA.

Motivos para renovação de certificado

Nada a assinalar.

Quem pode submeter o pedido de renovação de certificado

Nada a assinalar.

Processamento do pedido de renovação de certificado

Nada a assinalar.

Notificação de emissão de novo certificado ao titular

Nada a assinalar.

Procedimentos para aceitação de certificado

Nada a assinalar.

Publicação de certificado após renovação

Nada a assinalar.

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 gera um novo par de chaves e submete o pedido para emissão de novo certificado que certifica a nova chave pública.

Para cada tipo de certificados, a respetiva 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 serviço), mantendo as respetivas chaves, havendo apenas alterações na informação do certificado.

Esta prática não é suportada pela MULTICERT TS CA.

Motivos para alteração do certificado

Nada a assinalar.

Quem pode submeter o pedido de alteração de certificado

Nada a assinalar.

Processamento do pedido de alteração de certificado

Nada a assinalar.

Notificação da emissão de certificado alterado ao titular

Nada a assinalar.

Procedimentos para aceitação de certificado alterado

Nada a assinalar.

Publicação do certificado alterado

Nada a assinalar.

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 ação 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 assumem este estado de forma irreversível, enquanto os certificados suspensos podem recuperar a sua validade.

Para cada tipo de certificado, a respetiva Política descreve o processo de suspensão e revogação.

Motivos para Revogação

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

1. Comprometimento ou suspeita de comprometimento da chave privada;
2. Perda da chave privada;
3. Inexatidões graves nos dados fornecidos;
4. Comprometimento ou suspeita de comprometimento da senha e acesso à chave privada (exemplo: PIN);
5. Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/*token* criptográfico);
6. Incumprimento por parte da EC MULTICERT ou titular das responsabilidades previstas na Política de Certificado e/ou DPC;
7. Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
8. Por resolução judicial ou administrativa;
9. Utilização do certificado para atividades abusivas;
10. Risco de comprometimento de chave (por exemplo, devido à fraqueza do algoritmo ou tamanho de chave);
11. Cessação de funções da EC emissora.

4.10 Serviços sobre o estado do certificado

Caraterísticas operacionais

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

Disponibilidade do serviço

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

Caraterísticas 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 MULTICERT TS CA só efetua a retenção da sua chave privada.

Políticas e práticas de recuperação de chaves

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

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

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

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

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 nesta DPC. Esta secção descreve sucintamente os aspetos de segurança, não técnicos, que possibilitam de modo seguro, realizar as funções de geração de chaves, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos, 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

Localização física e tipo de construção

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

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

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

a) Paredes em alvenaria, betão ou tijolo;

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

c) Inexistência de janelas;

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

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

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

Acesso físico ao local

Os sistemas da MULTICERT TS CA 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 será possível quando, previamente, se tenha alcançado os privilégios necessários do nível imediatamente anterior.

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

O acesso ao cartão de identificação vermelho obriga a um duplo controlo de autenticação de acesso individual. 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 respetivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respetivo cartão de acesso visível.

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

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

Exposição à água

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

Prevenção e proteção contra incêndio

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

- Sistemas de deteção e alarme de incêndio estão instalados nos vários níveis físicos de segurança,
- Equipamento fixo e móvel de extinção de incêndios estão disponíveis, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso,
- Procedimentos de emergência bem definidos, em caso de incêndio.

Salvaguarda de suportes de armazenamento

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

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

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

Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível deverão ser triturados antes da sua eliminação.

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível (através de formatação "segura" de baixo nível ou destruição física), antes dos mesmos serem eliminados. Equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Outros equipamentos de armazenamento (discos rígidos, tapes, ...) deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

Instalações externas (alternativa) para recuperação de segurança

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

5.2 Medida de segurança dos processos

A atividade 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.

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 oito Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticados, eventualmente pertencentes a diferentes Grupos de Trabalho.

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.

Grupo de Trabalho de Operação

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

As responsabilidades deste grupo são:

- 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 correção 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*.

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

Grupo de Trabalho de Autenticação

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

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

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

As responsabilidades deste grupo são:

- Definir todas as políticas da EC e garantir que se encontram atualizadas e adaptadas à realidade desta;
- Assegurar que as PC's da EC são suportadas pela DPC da EC;
- Assegurar que todos os documentos relevantes e relacionados, direta ou indiretamente, com o funcionamento da EC se encontram armazenados no Ambiente de Informação;
- Gerir o Ambiente de Autenticação;
- Gerir todas as palavras-passe não pessoais;
- Manter um inventário atualizado 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 atualizado 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;
- Registar a devolução dos *tokens* de autenticação usados pelos membros dos restantes grupos;
- Registar trocas de palavras-passe de autenticação usadas pelos membros dos restantes grupos;
- Registar a perca de *tokens* de autenticação, descrevendo adequadamente a situação que lhe deu origem;
- Registar sempre que uma palavra-passe de autenticação é comprometida, descrevendo adequadamente a situação que o originou;
- Avaliar os riscos de negócio resultantes da perca de um *token* ou o comprometimento de uma palavra-passe de autenticação;
- Tomar medidas ativas de modo a não comprometer cada Ambiente de Produção derivado da perca de um *token*, ou do comprometimento de alguma palavra-passe de autenticação;
- Avaliar pedidos de replicação de documentação;
- Assumir o papel de *Administrador de Segurança*, conforme definido no artigo 29º do Decreto Regulamentar n.º 25/2004.

Grupo de Trabalho de Auditoria

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

[5] Registando o seu valor

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exatidão dos processos e cerimónias da EC;
- Registar todas as operações sensíveis;
- Investigar suspeitas de fraudes procedimentais;
- Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;
- Registar todos os procedimentos passíveis de auditoria;
- Registar os resultados de todas as ações por si realizadas;
- Assumir o papel de Auditor de Sistema, conforme definido no artigo 29º do *Decreto Regulamentar n.º 25/2004*;
- Validar que todos os recursos utilizados são seguros;
- Verificar periodicamente a integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respetivos[6] e que estão devidamente identificados;
- Verificar periodicamente os registos/logs da EC;
- Gerir o Ambiente de Auditoria.

Grupo de Trabalho de Custódia

É responsável pela custódia de alguns artefactos sensíveis (*tokens* de autenticação, etc.), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições[7]. Note-se que, no sentido de melhorar os níveis de segurança, operacionalidade e continuidade de negócio da EC, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de artefactos. Este grupo deve fazer uso dos vários ambientes seguros disponibilizados para a guarda deste tipo de itens. Este grupo deve ter um mínimo de 2 (dois) membros.

As responsabilidades deste grupo são:

- Gerir o Ambiente de Custódia;
- Custódia de artefactos sensíveis (*tokens* de autenticação, etc.) usando os meios adequados que respondam às necessidades de segurança respetivas;
- 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.

Grupo de Trabalho de Operação de Registo

É responsável por assegurar a emissão, renovação, suspensão e revogação de certificados.

As responsabilidades deste grupo são:

- Assumir o papel de Administrador de Registo, conforme definido no artigo 29º do *Decreto Regulamentar n.º 25/2004*;
- Validar a documentação a ser entregue pelos titulares para emissão/revogação de certificados;
- Emitir Certificados caso este processo não esteja automatizado;
- Revogar/Suspender certificados, caso este processo não esteja automatizado.

[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

Grupo de Trabalho de Monitorização e Controlo

A missão deste grupo consiste na consolidação e análise da monitorização dos pontos de controlo de segurança de todos os recursos utilizados na MULTICERT TS CA, que podem dar origem a eventos, alarmes e incidentes.

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

As responsabilidades deste grupo são:

- Consolidar e analisar a monitorização dos recursos utilizados na MULTICERT TS CA;
- Garantir a melhoria contínua do "Processo de gestão de Incidentes" e a respetiva gestão operacional;
- Colaborar com o Grupo de Trabalho de Auditoria com o objetivo de promover ações de melhoria contínua;
- Monitorizar o funcionamento dos alarmes existentes;
- Fazer passagens a produção requeridas pela pré-produção;
- Monitorizar eventos, gerir alarmes e classificar incidentes;
- Definir, apoiar a implementação e a melhoria contínua de procedimentos para resposta a incidentes;
- Fazer passagens a produção requeridas pela pré-produção.

Grupo de Trabalho de Gestão

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

A missão do Grupo de Trabalho de Gestão assenta principalmente na tomada de decisões importantes e críticas ao bom funcionamento da MULTICERT TS CA, 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 ser constituído pelo mínimo de 4 (quatro) elementos.

As responsabilidades deste grupo são:

- Gerir o Ambiente de Gestão;
- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Autenticação;
- 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.

Número de pessoas exigidas por tarefa

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

Os procedimentos de controlo interno foram elaborados de modo a garantir um mínimo de 2 indivíduos autenticados para se ter acesso físico ou lógico aos equipamentos de segurança. O acesso ao *hardware* criptográfico da EC segue procedimentos estritos envolvendo múltiplos indivíduos autorizados a aceder-lhe durante o seu ciclo de vida, desde a receção e inspeção até à destruição física e/ou lógica do hardware. Após a ativação de um módulo com chaves operacionais, controlos adicionais de acesso são utilizados de modo a garantir que os acessos físicos e lógicos ao *hardware* só são possíveis com 2 ou mais indivíduos autenticados. Indivíduos com acesso físico aos módulos, não detêm as chaves de ativação e vice-versa.

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...	**Pode pertencer ao Grupo?**	**Monitorização e Controlo**	**Operação**	**Autenticação**	**Operação de Registo**	**Auditoria**	**Custódia**	**Gestão**
Monitorização e Controlo						✖	✖	✖
Operação				✖	✖	✖	✖	✖
Autenticação			✖			✖	✖	✖
Operação de Registo			✖			✖	✖	✖
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 efetuou 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 respetivas funções, como também a sua capacidade e disponibilidade para o fazer.

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.

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.

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 Pública;
b) Conceitos gerais sobre segurança da informação;
c) Formação específica para o seu papel dentro do Grupo de Trabalho;
d) Funcionamento do *software* e/ou *hardware* usado pela EC;
e) Política de Certificados e Declaração de Práticas de Certificação;
f) Recuperação face a desastres;
g) Procedimentos para a continuidade da atividade e,
h) Aspetos legais básicos relativos à prestação de serviços de certificação.

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

Frequência e requisitos para ações de reciclagem

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

- Sempre que existe qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto às EC,
- Sempre que são introduzidas alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos das EC.

Frequência e sequência da rotação de funções

Nada a assinalar.

Sanções para ações não autorizadas

Consideram-se ações não autorizadas todas as 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 ações não autorizadas ou que façam uso não autorizado dos sistemas.

Requisitos para prestadores de serviços

Consultores ou prestadores de serviços independentes tem permissão de acesso à zona de alta segurança desde de que estejam sempre acompanhados e diretamente supervisionados pelos membros do Grupo de Trabalho e após tomada de conhecimento e aceitação da Declaração de Confidencialidade para Colaborador Externo ou Visitante[9], existente para o efeito.

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

Tipo de eventos registados

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

- Pedido, emissão, renovação, reemissão 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,

[9] MULTICERT_PJ.CA3_28_0001_pt.pdf - Declaração de Confidencialidade para Colaborador Externo ou Visitante

- 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.

Frequência da auditoria de registos

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

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.

Proteção dos registos de auditoria

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

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

Procedimentos para a cópia de segurança dos registos

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

Sistema de recolha de registos (Interno / Externo)

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

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.

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

Tipo de dados arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 0), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

Período de retenção em arquivo

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

Proteção dos arquivos

O arquivo:

- É protegido para que apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo,
- É protegido contra qualquer modificação ou tentativa de o remover,
- É protegido contra a deterioração do media onde é guardado, através de migração periódica para media novo,
- É protegido contra a obsolescência do hardware, sistemas operativos e 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,
- É guardado de modo seguro em ambientes externos seguros.

Procedimentos para as cópias de segurança do arquivo

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

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.

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

Os sistemas de recolha de dados de arquivo são internos.

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 do seu restauro.

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.

Procedimentos em caso de incidente ou comprometimento

Cópias de segurança das chaves privadas da EC (geradas e mantidas de acordo com a secção 0) e dos registos arquivados (secção 0) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

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

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

Se for confirmado que os recursos informáticos, *software* e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a MULTICERT TS CA suspenderá os seus serviços e notificará a Autoridade Credenciadora.

Procedimentos em caso de comprometimento da chave privada da entidade

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

- Revogação do certificado da MULTICERT TS CA e de todos os certificados emitidos no "ramo" da sua hierarquia de confiança,
- Notificação da Autoridade Credenciadora e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT TS CA,
- Geração de novo par de chaves para a MULTICERT TS CA,
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT TS CA.

Capacidade de continuidade da atividade em caso de desastre

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

5.8 Procedimentos em caso de extinção de EC ou ER

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

a) Informar a Autoridade Credenciadora;

b) Informar todos os titulares de certificados;

c) Revogar todos os certificados emitidos;

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

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

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

6 MEDIDAS DE SEGURANÇA TÉCNICAS

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

6.1 Geração e instalação do par de chaves

A geração dos pares de chaves da MULTICERT TS CA são processados de acordo com os requisitos e algoritmos definidos nesta política.

Geração do par de chaves

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

O *hardware* criptográfico, usado para a geração de chaves da MULTICERT TS CA, cumpre os requisitos FIPS 140-1 nível 3 e/ou *Common Criteria EAL* 4+ e, efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o *hardware*. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores. As cópias de segurança de chaves criptográficas são efetuadas apenas usando *hardware*, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perca de dados, possa haver uma recuperação total e segura das chaves.

A chave privada para os certificados de pessoa singular e de pessoa coletiva são gerados pela MULTICERT TS CA, usando *hardware* criptográfico que cumpre os requisitos FIPS 140-1 nível 3 e/ou *Common Criteria EAL* 4+.

O funcionamento da MULTICERT TS CA é efetuado em modo *on-line*.

Entrega da chave privada ao titular

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

Entrega da chave pública ao emissor do certificado

A chave pública é entregue à MULTICERT TS CA, de acordo com os procedimentos indicados na secção 4.3.

Entrega da chave pública da EC às partes confiantes

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

Dimensão das chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização. A dimensão das chaves é a seguinte:

- 4096 bits RSA para a chave da MULTICERT TS CA,
- 2048 bits RSA para as chaves associadas aos certificados emitidos pela MULTICERT TS CA, com algoritmo de assinatura sha256RSA

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#11.

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

De acordo com secção 7.1.

6.2 Proteção da chave privada e características do módulo criptográfico

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

Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da MULTICERT TS CA, 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 fatores
- 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
  - SHA-256
  - 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

Controlo multi-pessoal (n de m) para a chave privada

O controlo multipessoal 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 efetuar operações criptográficas sensíveis na EC.

Os dados de ativação necessários para a utilização da chave privada da MULTICERT TS CA 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 número de partes (m) é necessário para ativar a chave privada da MULTICERT TS CA guardada no módulo criptográfico em *hardware*. São necessárias duas (n) partes para a ativação da chave privada da MULTICERT TS CA.

Retenção da chave privada (key escrow)

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

Cópia de segurança da chave privada

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

Arquivo da chave privada

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

Transferência da chave privada para/do módulo criptográfico

As chaves privadas da MULTICERT TS CA 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 MULTICERT TS CA para um outro *token* criptográfico, essa cópia é feita diretamente, *hardware* para *hardware*, de uma forma que garante o transporte das chaves entre módulos numa transmissão cifrada.

Armazenamento da chave privada no módulo criptográfico

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

Processo para ativação da chave privada

A MULTICERT TS CA é uma EC *on-line*, cuja chave privada é ativada quando o sistema da EC é ligado. Esta ativação é efetivada através da autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação de dois fatores (consola de autenticação portátil e chaves PED – pequenos *tokens* de identificação digital, com o formato de 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 efetuar a cópia de segurança.

Para a ativação das chaves privadas da MULTICERT TS CA é necessária, no mínimo, a intervenção de quatro elementos do Grupo de Trabalho. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

Processo para desativação da chave privada

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

Para a desativação das chaves privadas da MULTICERT TS CA é necessária, no mínimo, a intervenção de quatro elementos do Grupo de Trabalho. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

Processo para destruição da chave privada

As chaves privadas da MULTICERT TS CA (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.

Avaliação/nível do módulo criptográfico

Descrito na secção 0.

6.3 Outros aspetos da gestão do par de chaves

Arquivo da chave pública

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

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 certificados e período em que os mesmos devem ser renovados, é o seguinte:

- O certificado da MULTICERT TS CA 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 OCSP e TSA por ela emitidos têm uma validade máxima de seis anos e 4 meses, sendo utilizados durante os seus 4 primeiros meses de validade e reemitidos a cada 4 meses;

6.4 Dados de ativação

Geração e instalação dos dados de ativação

Os dados de ativação necessários para a utilização da chave privada da MULTICERT TS CA 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 ao 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.

Proteção dos dados de ativação

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

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

Outros aspetos dos dados de ativação

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

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

6.5 Medidas de segurança informáticas

Requisitos técnicos específicos

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

A MULTICERT TS CA e o SGCVC dispõem de dispositivos de proteção 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.

Avaliação/nível de segurança

Os vários sistemas e produtos utilizados pela MULTICERT TS CA são fiáveis e protegidos contra modificações.

O módulo criptográfico em *Hardware* da MULTICERT TS CA 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

Medidas de desenvolvimento do sistema

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

É fornecida uma metodologia auditável que permite verificar que o *software* da MULTICERT TS CA 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.

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 MULTICERT TS CA, 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.

Ciclo de vida das medidas de segurança

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

6.7 Medidas de Segurança da rede

A MULTICERT TS CA dispõe de dispositivos de proteção 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. Todas estas entradas são assinadas digitalmente por um certificado emitido para o efeito.

7 PERFIS DE CERTIFICADO, CRL, E OCSP

7.1 Perfil de Certificado

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

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

- Recomendação ITU.T X.509[10],
- 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 0.

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 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].

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

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[10],
- 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 MULTICERT TS CA (de acordo com tabela da secção 0).

7.3 Perfil OCSP

O perfil dos certificados OCSP está de acordo com:

- Recomendação ITU.T X.509[10],
- 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 0.

8 AUDITORIA E AVALIAÇÕES DE CONFORMIDADE

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

Para além de auditorias de conformidade, a MULTICERT irá efetuar outras fiscalizações e investigações para assegurar a conformidade da MULTICERT TS CA 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[11]. 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

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[12]. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Autoridade Credenciadora podem ser encontrados em http://www.gns.gov.pt/media/3992/ListagemdeAS.pdf.

8.3 Relação entre o auditor e a Entidade Certificadora

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

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

O Auditor e a parte auditada (Entidade Certificadora) não devem ter nenhuma relação, atual 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 proteção 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).

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

[12] 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

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 final 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 final de auditoria à Autoridade Credenciadora e simultaneamente para os responsáveis da entidade auditada para apreciação;

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

f) 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 atividade seja desenvolvida até à próxima inspeção;

    b. Permitem que a entidade continue em atividade por um período máximo de 60 dias até à correção das irregularidades antes da revogação;

    c. Revogação imediata da atividade.

8.6 Comunicação de resultados

Os resultados devem ser comunicados ao auditor em causa e à Entidade Credenciadora.

9 OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

9.1 Taxas

Taxas por emissão ou renovação de certificados

Nada a assinalar.

Taxas para acesso a certificado

Nada a assinalar.

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

Nada a assinalar.

Taxas para outros serviços

Nada a assinalar.

Política de reembolso

Nada a assinalar.

9.2 Responsabilidade financeira

Seguro de cobertura

Nada a assinalar

Outros recursos

Nada a assinalar.

Seguro ou garantia de cobertura para utilizadores

Nada a assinalar

9.3 Confidencialidade da informação processada

Âmbito da confidencialidade da informação

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

a) As chaves privadas da MULTICERT TS CA;

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

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

d) Planos de continuidade de negócio e recuperação;

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

f) Informação de todos os documentos relacionados com a MULTICERT TS CA (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 MULTICERT TS CA 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 MULTICERT TS CA;

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

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

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

Responsabilidade de proteção da confidencialidade da informação

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

9.4 Privacidade dos dados pessoais

Medidas para garantia da privacidade

A MULTICERT tem implementadas medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa.

Informação privada

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

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.

Responsabilidade de proteção da informação privada

De acordo com a legislação portuguesa.

Notificação e consentimento para utilização de informação privada

De acordo com a legislação portuguesa.

Divulgação resultante de processo judicial ou administrativo

Nada a assinalar.

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 MULTICERT TS CA 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

Representação e garantias das entidades certificadoras

A MULTICERT TS CA 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 MULTICERT TS CA, com a frequência estipulada na secção 4.9.,

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

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

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

p) Operar de acordo com a legislação aplicável,

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

r) Garantir a disponibilidade da LRC de acordo com as disposições da secção 4.9.,

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

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

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

v) Disponibilizar os certificados da MULTICERT TS CA.

Representação e garantias das Entidades de Registo

Nada a assinalar.

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 Políticas 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.,

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

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

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

Representação e garantias das partes confiantes

É obrigação das partes que confiem nos certificados emitidos pela MULTICERT TS CA:

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

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

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

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

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

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 MULTICERT TS CA publique no seu sítio Web.

Representação e garantias de outros participantes

Nada a assinalar.

9.7 Renúncia de garantias

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

9.8 Limitações às obrigações

A MULTICERT TS CA:

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

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

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

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

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

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

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

h) A MULTICERT TS CA 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 Política de Certificados e correspondente DPC,

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

9.9 Indemnizações

De acordo com a legislação em vigor

9.10 Termo e cessação da atividade

Termo

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

Esta DPC entra em vigor assim que publicada no repositório da MULTICERT TS CA e manter-se-á, enquanto não for expressamente revogada, pela emissão de uma nova versão ou pela renovação das chaves da MULTICERT TS CA, momento em que obrigatoriamente se redigirá uma nova versão.

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 MULTICERT TS CA (incluindo esta DPC) quando:

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

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

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

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

Consequências da cessação de atividade

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

As obrigações e restrições que estabelece esta DPC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da MULTICERT TS CA, 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 eletrónico assinado digitalmente, fax, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação.

9.12 Alterações

Procedimento para alterações

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

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

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

Prazo e mecanismo de notificação

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

Motivos para mudar de OID

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

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

No caso em que o Grupo de Trabalho de Autenticação julgue que as alterações à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 0.

9.13 Disposições para resolução de conflitos

Todas as reclamações entre utilizadores e MULTICERT TS CA 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 atividade das entidades certificadoras a seguinte legislação específica:

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

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

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

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

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

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

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

9.15 Conformidade com a legislação em vigor

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

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

9.16 Providências várias

Acordo completo

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

Independência

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

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

Severidade

Nada a assinalar.

Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

Força Maior

Nada a assinalar.

9.17 Outras providências

Nada a assinalar.

10 Definições e acrónimos

Acrónimos

Acrónimo	Descrição
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 Objeto
PC	Política 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

Definições

Definição	
Assinatura digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura eletrónica	Resultado de um processamento eletrónico de dados, suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Assinatura eletrónica avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade Credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.

Certificado qualificado	Certificado que contém os elementos referidos no artigo 29.º do DL 62/2003 e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24.º do DL 62/2003.
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos.
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica.
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que: i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis;

	iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Entidade certificadora	Entidade ou pessoa singular ou coletiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respetiva publicidade e presta outros serviços relativos a assinaturas eletrónicas.
Organismo de certificação	Entidade pública ou privada competente para a avaliação e certificação da conformidade dos processos, sistemas e produtos de assinatura eletrónica 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 eletrónica	Suporte lógico, dispositivo de equipamento ou seus componentes específicos, destinados a ser utilizados na prestação de serviços de assinatura eletrónica qualificada por uma entidade certificadora ou na criação e verificação de assinatura eletrónica qualificada.
Titular	Pessoa singular ou coletiva 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 receção de um documento eletrónico.

Conclusão

Este documento define os procedimentos e práticas utilizadas pela MULTICERT *Trust Services Certification Authority*, no suporte à sua atividade de certificação digital. A hierarquia de confiança da MULTICERT *Trust Services Certification Authority*:

- Fornece uma hierarquia de confiança, que promoverá a segurança eletrónica do titular dos certificados no seu relacionamento com terceiras partes,
- Proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações 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.

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

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).

ETSI TS 102 042; *Policy requirements for certification authorities issuing public key certificates, v2.4.1*.

Ca/Browser Forum – Baseline Requirements, v1.3.3.

Aprovação

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

Assinado de forma digital por [Assinatura Qualificada]
MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Dados: 2016.04.04 09:03:12 +01'00'

X

Jorge Alcobia
Grupo de Trabalho de Gestão