TEC/1

Certification Practice Statement - MULTICERT CA

Documento: Certification.Practice.Statement.CA.TEC-0.v2.doc

Classificação: Público

Versão: 0.2.3

Data de criação: 26/01/2001

Data de impressão: 21/04/2003

Impresso para: - destinatários -

MULTICERT – Serviços de Certificação Electrónica S.A., Polo Tecnológico de Lisboa, CID - Lote 1 1600-546 LISBOA . PORTUGAL

Telefone: 217 123 010 Facsimile: 217 123 011

0 Estado do Documento

Autor(es):	Luis Vitor Carvalho Felix	26/01/2001
		Data
Verificado por:		
		Data
Aprovado por:		
		Data

0.1 Revisão

Este documento deverá ser revisto até 1 ano após a sua aprovação/verificação.

0.2 Identificação do Documento

Referência do Documento	Gestão Documental	Versão actual	Nome do Ficheiro	Data de criação
TEC/RFC/01	MULTICERT	0.2.3	Certification.Practice.Statement.CA.TEC-0.v2.doc	26/01/2001

0.3 História das Versões

Versão Nº	Data	Detalhes	Autor
0.1	26/01/2001	Draft inicial	Luis Felix
0.2	15/07/2002	Enquadramento no âmbito da MULTICERT S.A.	José Pina Miranda
0.2.1	23/07/2002	Alteração de secção 3.3.1.1	José Pina Miranda
0.2.2	10/02/2003	Alterações ligeiras indicadas por Pedro Borges	José Pina Miranda
0.2.3	21/04/2003	Adição de termos ao glossário e resolução de inconsistência na secção 7.1	José Pina Miranda

As alterações estão devidamente assinaladas com uma linha vertical na margem direita.

1 Sumário Executivo

1.1 Objectivos do Documento

O objectivo deste documento é definir os procedimentos e práticas levadas a cabo pela MULTICERT CA no desenrolar da sua actividade de certificação digital. Este documento é referido como sendo o *Certification Practice Statement* (CPS) da MULTICERT CA.

1.2 Âmbito do Documento

Este documento descreve os processos praticados pela MULTICERT para gerir e manter a Autoridade de Certificação MULTICERT CA.

Os procedimentos são descritos para cada etapa do ciclo de vida dos certificados emitidos, bem como outros aspectos que digam respeito à segurança e credibilidade da MULTICERT CA.

Este documento faz parte das Regras Políticas da MULTICERT.

1.3 Leitores

Este documento deverá estar disponível publicamente e é destinado a todas as entidades que se relacionem de alguma forma com a MULTICERT ROOT CA.

1.4 Referências Bibliográficas

1.5 Glossário

Termo	**Significado**
CA	Certification Authority – ver Entidade certificadora.
Certification Policy	Conjunto de regras que define a aplicabilidade de um certificado digital no contexto de uma determinada comunidade de Clientes, ou classe de aplicações.
CPS	*Certificate Practice Statement* – Documento ou conjunto de documentos onde se enunciam as práticas de certificação empregues pela entidade certificadora no processo de gestão de certificados.

Termo	**Significado**
CRL	*Certification Revocation List* – Documento mantido e publicado pela Entidade certificadora (EC) que identifica os certificados emitidos pela EC e que já não são válidos.
Entidade certificadora	Entidade que cria ou fornece meios para a criação e verificação das assinaturas digitais, emite e gere o ciclo de vida dos certificados digitais, assegura a respectiva publicidade e presta outros serviços relativos a assinaturas electrónicas.
Entidade de Certificação	Ver Entidade certificadora.
ER	Entidade de Registo – Entidade que presta à MULTICERT os serviços relativos à celebração de Contratos de Emissão de Certificado Digital de Cliente e à gestão de certificados digitais que não se encontrem, por lei ou por contrato, atribuídos em exclusivo à MULTICERT.
FIPS	*Federal Information Processing Standards* – conjunto de standards dos EUA que descrevem o processamento de documentos e algoritmos informáticos.
OID	*Object IDentifier* – sequência de números alocados de um modo hierárquico usados em vários protocolos (a MULTICERT é a autoridade para o OID cujo topo hierárquico é o 1.3.6.1.4.1.6204). A definição formal de um OID está expressa no capítulo 28 da recomendação ITU-T X.208 (ASN.1).
PKI	*Public Key Infrastructure* – uma infra-estrutura (constituída por software, hardware, procedimentos, pessoal, documentação, etc.) que governa e gere a utilização da criptografia de chave pública.
RA	*Registration Authority* – ver ER

Índice

2 Introdução

2.1 Aplicabilidade

2.1.1 A MULTICERT

A MULTICERT, enquanto autoridade de certificação, cumpre as disposições previstas no Decreto-Lei 290-D/99, assumindo as competências aí descritas e é responsável por fornecer serviços e assegurar os procedimentos (mesmo que recorrendo à subcontratação de terceiras partes) que possam garantir as seguintes funcionalidades a seguir indicadas:

1. Geração do seu próprio par de chaves criptográficas e geração do pedido de certificação para a sua chave pública.

2. Recepção e validação dos pedidos de emissão de certificados realizados pelos utilizadores finais (i.e. serviço de registo).

3. Emissão de certificados para utilizadores finais, relativos a pedidos de certificados que estejam de acordo com o formato requerido pela entidade de certificação MULTICERT CA.

4. Recepção e validação dos pedidos de suspensão, reactivação e revogação de certificados de utilizadores finais.

5. Publicação dos certificados dos utilizadores finais (quando e onde for apropriado) e de informação acerca do seu estado.

6. Assegurar a contínua disponibilidade da informação pública para todos os seus utilizadores.

7. Solicitação da revogação do seu próprio certificado, à entidade de certificação emissora do certificado da MULTICERT CA.

2.1.2 A Entidade de Registo

A Entidade de Registo (ER) é uma entidade autorizada a reunir e verificar informação de identidade de utilizadores e a informação exigida pela MULTICERT. A MULTICERT poderá agir como ER e/ou estabelecer acordos com outras entidades para que estas desempenhem também esse papel.

2.1.3 Aplicabilidade

Os certificados emitidos pela MULTICERT CA não poderão ser utilizados para efeitos de certificação cruzada e/ou hierárquica.

2.1.4 Contacto

O contacto da MULTICERT para todos os efeitos é, por carta:

MULTICERT
Polo Tecnológico de Lisboa, CID - Lote 1
1600-546 Lisboa
Portugal

por correio electrónico:

info@multicert.com

por telefone:

(+351) 217 123 010 (geral)

(+351) 217 123 012 (suporte)

ou por fax:

(+351) 217 123 011.

3 Definições Gerais

3.1 Deveres e Obrigações

3.1.1 Da Autoridade de Certificação

A MULTICERT CA, enquanto Autoridade de Certificação, cumpre as disposições previstas no Decreto-Lei Nº 290-D/99, assumindo as competências aí descritas e que incluem:

1. A emissão, renovação e revogação dos certificados digitais MULTICERT CA.

2. Fornecimento dos meios técnicos necessários à criação dos pares de chaves e do certificado, com rigorosa observância do disposto, zelando pela correspondência funcional entre os pares de chaves e pela exactidão das informações constantes dos certificados.

3. A observação de todas as regras de segurança na emissão, renovação e revogação dos certificados.

4. A manutenção do serviço de disponibilização do estado dos certificados.

5. A notificação dos requerentes, por correio electrónico ou por carta, de modo completo e claro, sempre que se procedam a operações de emissão, renovação, suspensão ou revogação dos certificados, tanto da própria MULTICERT CA como dos indivíduos por ela certificados.

6. A notificação dos subscritores de certificados, sempre que se introduzam alterações no processo de certificação ou nos requisitos técnicos necessários para ter acesso ao mesmo, que não fizessem parte do contrato estabelecido à data de realização do mesmo. A notificação será feita com uma antecedência de 30 dias por correio electrónico, ou por carta.

7. A publicação de uma versão actualizada deste documento no repositório público de informação <http://www.multicert.com/CPS/MULTICERT-CA-CPS.html>.

8. Cumprimento rigoroso das regras de segurança para tratamento de toda a informação recolhida e armazenada pela MULTICERT, no âmbito dos processos de identificação e autenticação ou de emissão dos certificados, tal como é definido pelo Decreto-Lei Nº 67/98 relativo à protecção de dados pessoais informatizados.

9. A publicação das chaves públicas e respectivos certificados, bem como a prestação de informação sobre a validade dos mesmos a qualquer pessoa ou entidade que o solicite, por meio electrónico adequado e expedito.

3.1.2 Da(s) Entidade(s) de Registo

Todas as entidades de registo reconhecidas pela MULTICERT, são responsáveis pelo cumprimento escrupuloso das normas e procedimentos de identificação/autenticação dos requerentes referenciados neste CPS.

As entidades de registo devem por isso garantir a correcta identificação dos subscritores que a ela se dirigem, verificando a autenticidade da documentação apresentada e/ou utilizando quaisquer outros métodos alternativos aprovados pela MULTICERT CA.

As entidades de registo têm a obrigação de manter registos detalhados de toda a sua tarefa e assegurar a escrupulosa segregação de funções entre os seus funcionários, de acordo com o que se define neste CPS.

A entidade de registo é ainda responsável pela conservação segura da sua chave privada por forma a que possam ser devidamente autenticadas e mantidas sob regime de confidencialidade todas as comunicações entre a mesma e a entidade de certificação MULTICERT CA.

Cada entidade de registo assume também a responsabilidade sobre a confidencialidade dos formulários e cópias de documentos que lhe são entregues durante o processo de identificação/autenticação dos subscritores deste serviço, devendo arquivá-las em local seguro durante o prazo imposto por lei.

3.1.3 Dos Requerentes e/ou Subscritores de Certificados Emitidos pela MULTICERT CA

Os requerentes estão obrigados a respeitar na íntegra as condições do contrato estabelecido com a MULTICERT no momento do registo, tendo em particular atenção o âmbito definido para a utilização do certificado posteriormente obtido. Neste sentido está expressamente proibida qualquer utilização de um certificado emitido pela MULTICERT CA que não esteja compreendida na respectiva *Certificate Policy*.

O requerente fica igualmente obrigado a proteger a sua chave privada e a notificar a MULTICERT CA assim que existam suspeitas de que essa chave possa estar comprometida. O não cumprimento desta prerrogativa desobriga a entidade de certificação de qualquer responsabilidade pela utilização indevida ou incorrecta do certificado emitido.

3.1.4 Das terceiras partes que recebem documentos assinados digitalmente com certificados emitidos pela MULTICERT CA

Todas as entidades que recebam documentos assinados digitalmente com um certificado emitido pela MULTICERT CA estão obrigadas a confirmar a sua validade, e a validade da cadeia de certificados a ele relativa, através de um dos serviços disponíveis para o efeito (CRL e/ou OCPS), sem o que, a sua aceitação, passa a constituir um acto da exclusiva responsabilidade da entidade aceitante.

3.2 Responsabilidade Financeira

A entidade de certificação assume a responsabilidade pelos danos causados a um terceiro que decorra directamente da utilização de um certificado danificado, emitido pela MULTICERT CA, por vias de falha técnica no processo de emissão, desde que o certificado não tivesse sido já suspenso ou revogado na altura da sua utilização.

Cabe às entidades de registo a responsabilidade pelos danos causados a um terceiro que decorram directamente da deficiente realização do processo de registo e identificação, desde que o certificado não tivesse sido já revogado na altura da sua utilização.

3.3 Limite de Responsabilidades

3.3.1 Responsabilidade da MULTICERT

A MULTICERT é responsável pela exactidão da informação nos certificados, no sentido de garantir a todas as entidades que depositam a sua confiança num certificado por ela emitido, que o mesmo foi passado para o denominado subscritor, que a informação no certificado está correcta e que o subscritor aceitou o certificado.

A MULTICERT é responsável por fornecer informações sobre o estado dos certificados emitidos.

A MULTICERT CA será responsável perante os utilizadores finais, se proceder a uma revogação de um certificado em circunstâncias em que não tenha autorização para tal, A NÃO SER QUE consiga provar que o pedido de revogação foi válido, mesmo que não cumpra os requisitos de revogação razoáveis ou quando os requisitos não são razoavelmente suficientes;

A MULTICERT é responsável por manter registos com informação sobre os certificados de forma a poder identificar positivamente tanto as entidades subscritoras dos mesmos como o histórico das relações com estas.

3.3.1.1 Exclusão da responsabilidade da MULTICERT CA

A MULTICERT não será, salvo o devidamente especificado abaixo, responsável por qualquer perda ou danos sofridos por partes que nela confiem, quando estas sejam derivadas dos seguintes motivos:

- perda ou compromisso da chave privada da MULTICERT CA, **A NÃO SER** que a MULTICERT CA não tenha cumprido os requisitos de gestão de chaves a que está obrigada, caso em que a MULTICERT CA será (sujeita a quaisquer outras restrições ou exclusões, especificadas abaixo) responsável para com a parte que nela confia, até ao limite de danos que esta seja capaz de provar serem responsabilidade da MULTICERT CA e dentro dos limites acima estabelecidos,

- qualquer informação incorrecta contida num Certificado de Identidade emitido

pela MULTICERT CA, **A NÃO SER** que a MULTICERT CA não tenha usado todos os meios razoáveis para garantir a precisão e correcção dessa informação, **OU** que a MULTICERT CA tenha falhado na verificação da autenticidade de todas as provas documentais dessa informação, caso em que a MULTICERT CA será (sujeita a quaisquer outras restrições ou exclusões, especificadas abaixo) responsável perante a parte que nela confia até ao limite de danos que esta seja capaz de provar serem responsabilidade da MULTICERT CA e dentro dos limites acima estabelecidos,

- a confiança que as partes que nela confiam tenham em certificados emitidos pela MULTICERT CA, quando a essas partes não verificarem o estado destes junto do serviço de informação de estado disponibilizado pela MULTICERT CA,

- a confiança que as partes que nela confiam tenham num certificado emitido pela MULTICERT CA, após essas partes terem verificado, junto do serviço de informação de estado disponibilizado pela MULTICERT CA, que o certificado se encontra revogado/suspenso e ainda assim tenham decidido confiar no mesmo,

- a indisponibilidade da informação de estado acerca dos certificados, por motivos de falhas de comunicação ou outras às quais a MULTICERT seja alheia,

- quaisquer dados incorrectos contidos na informação de estado dos certificados MULTICERT CA, **A NÃO SER** que a MULTICERT CA não faça a actualização dessa informação conforme os procedimentos a que está obrigada. Nesse caso a MULTICERT CA será (sujeita a quaisquer outras restrições ou exclusões, especificadas abaixo) responsável perante a parte que nela confia até ao limite de danos que esta seja capaz de provar serem responsabilidade da MULTICERT CA e dentro dos limites acima estabelecidos,

- qualquer falha, de outra parte qualquer, em cumprir com qualquer uma das obrigações estabelecidas para com a parte que nela confia,

- Qualquer perda ou compromisso da chave privada de uma entidade abaixo na sua hierarquia.

Em quaisquer circunstâncias, a MULTICERT CA não será responsável por:

- quaisquer danos indirectos ou por consequência;
- quaisquer perdas de lucros;
- quaisquer perdas de boa-vontade;
- quaisquer perdas de poupanças antecipadas;
- quaisquer perdas de receitas;
- quaisquer perdas de negócios;
- quaisquer interrupções de negócios; ou
- perdas de informação.

3.3.1.2 Limitações da responsabilidade da MULTICERT

Caso a MULTICERT seja considerada responsável, perante uma parte que nela confia e nas condições acima descritas, essa responsabilidade para com essa parte, assumida pela MULTICERT e respectivas Autoridade de Registo, não ultrapassará em quaisquer circunstâncias:

- no que diz respeito a cada reclamação individual, a soma total constante em cada Certificado de Identidade relevante em que a parte que nele confia tenha confiado ou 10,000 Euro (qualquer que seja o menor); e
- no que diz respeito a todas as reclamações em agregado realizadas à autoridade de certificação num ano, repartível por todas as responsabilidades emergentes da sua actividade, uma soma de 125,000 Euro.

Sobrepõem-se contudo a estas limitações o nº2 do Artigo 27 do Decreto-Lei Nº 290-D/99.

Ainda, nenhuma reclamação poderá ser considerara mais do que uma vez por toda a hierarquia da MULTICERT.

3.3.1.3 Eventos de Força Maior

Se a MULTICERT CA for impedida ou retardada no realizar de quaisquer uma das suas obrigações por um Evento de Força Maior ou por Causas Naturais, então a MULTICERT CA não será responsável por:

- qualquer falha ou atraso para executar quaisquer obrigações até ao limite da falha que for resultado do Evento de Força Maior ou de Causa Natural; e
- qualquer perda ou danos de qualquer natureza sofridos por, queixas de qualquer natureza feitas contra, ou custos de qualquer natureza contraídos pelas partes que nela confiam derivados de tal falha ou atraso por parte da MULTICERT CA para executar as obrigações afectadas pelo Evento de Força Maior ou de Causa Natural.

3.3.1.4 Limitações da exclusão da MULTICERT CA ou limitação de responsabilidade

Nada neste documento limitará ou excluirá a responsabilidade da MULTICERT CA pelo seguinte:

- Morte ou ferimentos pessoais resultantes de negligência por parte da MULTICERT CA; ou
- fraude interna.

3.3.2 Responsabilidade das ERs

A responsabilidade das Entidade de Registo, nessa capacidade, está incluída no que está descrito abaixo:

- Onde a ER não seguir o seu próprio processo de autenticação, assumirá a responsabilidade perante as partes que nela confiam;

- Se quaisquer documentos forjados forem apresentados à ER por um possível utilizador final e caso esta os tenha aceite, sem usar métodos razoáveis para verificar a autenticidade desses documentos (é de notar que a ER apenas terá de assumir a responsabilidade por agir na documentação forjada onde não conseguir estabelecer razoavelmente que os documentos foram forjados);

- Onde os documentos requisitados não identifiquem, sem qualquer dúvida, a identidade do pretendente subscritor;

- A ER será obrigada a especificar nos seus acordos com os utilizadores finais que os vários meios de validação de certificados da MULTICERT CA, podem ser retirados da rede em situações de emergência, de forma a proteger a integridade da infra-estrutura MULTICERT. Terão também de acordar com os utilizadores finais que estes não aceitarão qualquer certificado a não ser que seja possível saber a sua informação de estado através de um serviço publicamente disponível.

3.3.3 Lei pela qual se rege

Este documento rege-se, e deverá ser observado pela lei da República Portuguesa.

3.3.4 Resolução de disputas

Fica desde já definido o Tribunal Cível da Comarca de Lisboa.

3.4 Preços

Os preços actualizados para cada tipo de certificados emitidos ao abrigo das considerações mencionadas no presente CPS, são publicados em preçário periodicamente emitido pela MULTICERT ou estabelecidos por contracto com os subscritores e entidades que nela confiam. Note-se que os preços referidos são preços gerais por certificado, sujeitos a descontos que dependem da quantidade e do objectivo para que se destinam.

Se, no prazo de 30 dias, a contar da data de emissão do certificado, o requerente solicitar à MULTICERT CA a sua devolução por motivo de falha técnica comprovável, o certificado será revogado e o requerente reembolsado pelo valor pago e sem quaisquer custos adicionais perante a garantia de não uso do mesmo e das respectivas chaves criptográficas certificadas.

3.5 Auditoria

As práticas de certificação da MULTICERT são alvo de auditorias periódicas, que terão como mínimo a periodicidade estipulada na lei, ou seja, uma periodicidade anual com a emissão de um relatório à data de 31 de Março do ano civil em causa. Esta auditoria será realizada por uma entidade externa registada e reconhecida para o efeito. Esta auditoria é realizada tomando como base os *standards* de normalização existentes para o efeito sendo os

seus resultados comunicados à entidade credenciadora que poderá tornar público o resultado de todo o processo.

No sentido de cumprir com estas obrigações, a MULTICERT mantém registo de todas as operações do ciclo de vida dos certificados e de todas as comunicações mantidas com as entidades de registo/certificação por si reconhecidas. Da mesma forma, a MULTICERT obriga estas entidades a manter registo dos pedidos de subscrição recebidos e processados nos quais tenha estado envolvida. Este registo deverá ser mantido num repositório de dados criado para o efeito e deverá poder ser confirmada através da análise dos registos das comunicações (em suporte electrónico ou outro) com a entidade de certificação.

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

3.6 Direitos de Propriedade Intelectual e Industrial

Todos os Direitos de Propriedade Intelectual e Industrial deste documento, das *Certificate Policies* da MULTICERT CA, e dos Certificados Digitais emitidos pela mesma (incluindo informação sobre o seu estado) são propriedade da MULTICERT. Da mesma forma os logotipos, nomes, imagens, domínios e marcas próprias incorporadas nos Certificados Digitais emitidos pela MULTICERT CA são propriedade da MULTICERT. Todos os suportes físicos utilizados para armazenamento da informação dos certificados são também propriedade da MULTICERT.

3.7 Cessação da Actividade

No caso de existência de um processo de cessação de actividade por parte da entidade de certificação MULTICERT CA, estarão garantidos todos os direitos adquiridos dos subscritores dos certificados, aplicando-se para o efeito as disposições referidas no Decreto-Lei 290-D/99 de 2 de Agosto de 1999.

Nessa eventualidade a MULTICERT CA comunicará essa intenção a todos os subscritores de certificados válidos, com a antecipação mínima de três meses, indicando nesse momento qual a entidade que será fiel depositária de toda a documentação e que tratará de assumir os compromissos pela renovação e manutenção dos certificados. Neste contexto caberá à entidade reguladora do Estado Português a função de supervisão do processo de transferência de responsabilidades, documentação e infra-estrutura técnica.

4 Identificação e Autenticação

4.1 Registo Inicial

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

4.1.1 Tipos de Nomes

A MULTICERT CA garante a emissão de certificados contendo um *Distinguished Name* (DN) **X.500**. A MULTICERT CA assegurará, dentro da sua infra-estrutura de confiança, a não existência de certificados que contendo o mesmo DN possam identificar entidades distintas.

4.1.2 Necessidade de os Nomes Serem Significativos

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

4.1.3 Regras Para a Interpretação dos Vários Formatos de Nome

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

4.1.4 Unicidade dos Nomes

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

4.1.5 Resolução de Disputas de Nomes

A MULTICERT CA será responsável por atribuir e aprovar os DNs. Será também responsável por resolver quaisquer disputas que possam surgir.

4.1.6 Reconhecimento, Autenticação e Papeis das Marcas Registadas

Os nomes emitidos pela MULTICERT respeitarão no máximo possível as marcas registadas. A MULTICERT não permitirá deliberadamente a utilização de nomes registados cuja entidade não possa provar serem de sua propriedade. Contudo a MULTICERT poderá recusar a emissão de certificados com nomes de marcas registadas se entender que outra identificação é mais conveniente.

4.1.7 Método de Prova da Posse da Chave Privada

Nos casos em que a MULTICERT não seja a responsável pela geração do par de chaves criptográficas, a atribuir ao utilizador, a MULTICERT assegurará que o utilizador possui a chave privada correspondente à chave pública constante do pedido de certificado antes de proceder à sua emissão.

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

4.1.8 Autenticação da Identidade de Clientes

As entidades de registo reconhecidas pela MULTICERT serão responsáveis por autenticar a identidade dos clientes candidatos à obtenção de um certificado. As formas de proceder a essa autenticação incluem:

- Assegurar que o cliente existe e autorizou a emissão do certificado.
- Assegurar que os representantes legais da MULTICERT aceitaram o cliente em questão dentro da sua hierarquia.

O processo de registo e autenticação será assegurado pelo seguinte: é da responsabilidade da ER registar correctamente os utilizadores finais do certificado, usando todos os meios necessários para os identificar positivamente e de forma legal. Entre as operações a realizar para atingir este objectivo contam-se:

1. verificar em documentos oficialmente reconhecidos pelo Estado em que o subscritor (individual ou organização) está registado:

   a) o nome completo.
   b) os dados de contacto, incluindo o endereço de contacto.
   c) o sua identificação única legal

2. garantir a presença física do subscritor no momento da realização do registo, a não ser que já exista uma relação de confiança com a ER previamente baseada nessa presença física do subscritor.

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

   1) O subscritor ou o seu representante legal (no caso de uma pessoa colectiva) deverão apresentar-se fisicamente numa ER reconhecida pela MULTICERT;
   2) A identificação física deverá ser autenticada contra provas identificativas que devem estar de acordo com as provisões seguintes:

(a) Ser oficialmente reconhecidas na jurisdição em que o subscritor está registado,

(b) Indicar o nome completo do subscritor, o seu endereço oficial,

(c) Ter pelo menos uma prova de identidade que contenha uma fotografia do subscritor (sempre que aplicável),

(d) Indicar um número de registo único dentro da jurisdição em que tiver sido emitido;

3) No caso de certificados para subscritores não humanos, os processos de autenticação referidos serão aplicados às pessoas que estejam autorizadas a pedir certificados para os subscritores especificados;

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

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

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

4.1.8.1 Acordo com o Subscritor

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

1. acordo das obrigações com o subscritor e do subscritor;
2. consentimento para a manutenção de registos por parte da MULTICERT, com a informação usada no registo, bem como informação de subsequentes acontecimentos relativos ao acordo e ao seu objecto;
3. permissão para passar esta informação a terceiros sob certas condições;
4. permissão para passar informação sobre o estado dos certificados emitidos, ao abrigo do acordo, a terceiros não descriminados.

4.1.8.2 Pedido lógico de Certificado

1. A MULTICERT CA exigirá que uma entidade requerente de um certificado prepare e submeta os dados apropriados ao pedido, como especificado neste CPS.

2. Quando necessário, a MULTICERT CA exigirá que a entidade final requisitante submeta à ER a sua chave pública para certificação, numa mensagem assinada digitalmente usando a chave privada a que corresponde a chave pública constante do pedido, de forma a:

   a) permitir a detecção de erros no processo de certificação, e

   b) provar a posse da chave privada relativa à chave pública a certificar.

3. A MULTICERT CA usa a chave pública contida no Pedido lógico de Certificado da entidade requisitante para verificar a assinatura da entidade requisitante no Pedido lógico de Certificado submetido.

4. A MULTICERT CA verifica a autenticidade da submissão, da ER, de acordo com este CPS.

5. A MULTICERT CA verificará a assinatura da ER no Pedido lógico de Certificado.

6. A MULTICERT CA verifica o Pedido lógico de Certificado para verificar se este contém erros ou omissões de acordo com este CPS.

7. A MULTICERT CA verifica a unicidade do *Distinguished Name* da entidade requisitante dentro da infra-estrutura da MULTICERT.

8. A MULTICERT CA aceita o Pedido lógico de Certificado vindo da entidade requisitante, cuja identidade foi validada.

9. Quando a MULTICERT CA detectar chaves públicas repetidas o Pedido lógico de Certificado é rejeitado.

4.1.9 Autenticação Presencial de Entidades Individuais

A autenticação presencial do representante autorizado das organizações candidatas a um certificado será baseada em, pelo menos, duas formas de identificação emitidas pelo governo (em que pelo menos uma terá de ser um documento com fotografia, tal como, um passaporte). A capacidade da pessoa agir em nome da organização candidata será também autenticada, através da apresentação de documentação em papel, indicando este facto.

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

4.2 Renovação de Rotina

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

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

1) O indivíduo/organização ainda existe e autorizou a emissão do certificado.

2) O indivíduo/organização continua a obedecer aos requisitos de associação.

3) O indivíduo/organização possui a chave privada correspondente à nova chave pública

expedida para certificação.

4) A MULTICERT aceita a continuidade do indivíduo/organização dentro da hierarquia MULTICERT.

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

4.3 Renovação Após Revogação

Se um certificado é revogado, o indivíduo/organização tem de fazer, de novo, todo o processo inicial de registo, de forma a obter um novo certificado. Porém, o *Certificate Policy* do certificado a renovar pode especificar expressamente outras condições de renovação, inclusive contrárias a esta.

4.4 Pedido de Revogação

O pedido de revogação deve obedecer às condições descritas em pormenor na secção 5.4.

5 Requisitos Operacionais

5.1 Pedido de Certificados

O pedido de certificados tanto pode ser iniciado *off-line* como através da Internet, estando para cada caso e conforme o tipo de certificado, publicados os procedimentos na respectiva *Certificate Policy*.

5.2 Emissão dos Certificados

A MULTICERT CA emite os certificados digitais recorrendo a *hardware* criptográfico que cumpre no mínimo os requisitos *FIPS-140 Level 2*.

5.3 Aceitação do Certificado

O contrato assinado aquando do pedido de certificado juntamente com a emissão do respectivo certificado digital, indica formalmente a aceitação do certificado e das regras e condições associadas a este.

5.4 Suspensão e Revogação de Certificados

5.4.1 Circunstâncias para Revogação

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

- A pedido por escrito do titular, devidamente identificado para o efeito.
- Comprometimento ou suspeita de comprometimento da chave privada do certificado.
- Sempre que alguma informação constante do certificado já não seja exacta.
- Perda da chave privada do certificado.
- Confirmação da emissão do certificado feita com base em informações erróneas ou falsas.
- Quando finde o prazo do certificado.
- Quando a ER ordenar a revogação do certificado por motivo legalmente fundado.
- Se a MULTICERT CA cessar as suas actividades sem ter transmitido a sua documentação a outra entidade de certificação.

- Como resultado do comprometimento ou terminação da chave privada da MULTICERT CA.

5.4.2 Quem pode solicitar a Revogação

As únicas partes que podem solicitar a revogação dos certificados emitidos pela MULTICERT CA são a MULTICERT, a ER responsável pela emissão do certificado e os titulares e/ou representantes legais da entidade/indivíduo a quem o certificado foi atribuído.

5.4.3 Procedimento para solicitação de Revogação

O procedimento a ser seguido por parte de um utilizador para solicitar a revogação do seu próprio certificado é o seguinte:

> O utilizador deverá contactar imediatamente a MULTICERT, ou uma das entidades referidas no respectivo *Certificate Policy*, logo que a decisão de pedir a revogação seja tomada.
>
> Durante o horário de expediente normal o número de contacto da empresa deverá ser usado, em qualquer outra altura o número telefónico de suporte deverá ser usado. A palavra-passe designada de PUK, previamente atribuída, deverá ser usada para autenticar o utilizador.
>
> O utilizador deverá também enviar à MULTICERT, de forma escrita e devidamente assinada, um pedido de revogação do certificado, incluindo o motivo para tal operação.

O procedimento a ser seguido pela MULTICERT para revogar o certificado é o seguinte:

> Após a recepção do pedido de revogação, o certificado será imediatamente suspenso, até os motivos para a revogação serem correctamente analisados e se poder chegar a alguma conclusão.
>
> Após análise da situação e dos motivos para a revogação, sendo este aprovado, proceder-se-á à finalização do processo que consistirá na alteração da informação do certificado para Revogado e na publicação de um anúncio da revogação.
>
> O subscritor será então notificado da alteração de estado do certificado.

5.4.4 Processamento do Pedido de Revogação

Após a recepção de um pedido telefónico de revogação, o certificado em questão passará ao estado de suspenso e essa informação será imediatamente publicada num prazo máximo de 120 minutos.

Uma vez aceite o pedido de revogação de um certificado, este será revogado imediatamente no prazo máximo de 30 minutos. Caso contrário o certificado não será revogado e deixará de estar suspenso.

5.4.5 Circunstâncias para Suspensão

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

- A pedido por escrito do titular, devidamente identificado para o efeito.
- Quando existam fundadas razões para crer que o certificado foi emitido com base em informações erróneas ou falsas.
- Quando as informações nele contidas deixarem de ser conformes com a realidade.
- Quando a confidencialidade da chave privada for violada.

É de notar que a suspensão é o primeiro passo para a revogação de um certificado. Caso as razões apresentadas para a suspensão sejam provadas dar-se-á, de seguida, início ao processo de revogação do certificado.

5.4.6 Quem Pode Pedir a Suspensão

As únicas partes que podem pedir a revogação dos certificados emitidos pela MULTICERT CA são a MULTICERT, a ER responsável pela emissão do certificado e os titulares e/ou representantes legais da entidade/indivíduo a quem o certificado foi atribuído.

5.4.7 Procedimento Para um Pedido de Suspensão

O procedimento a ser seguido por parte de um utilizador para pedir a suspensão do seu próprio certificado é o seguinte:

- O utilizador deverá contactar a MULTICERT imediatamente após a decisão de pedir a suspensão seja tomada. Durante o horário de expediente normal o número de contacto da empresa deverá ser usado, em qualquer outra altura o número telefónico de suporte deverá ser usado. A palavra-passe, designada de PUK, previamente atribuída deverá ser usada para autenticar o utilizador.

O utilizador deverá também enviar por fax, à MULTICERT, uma cópia completa do pedido de suspensão, incluindo o motivo para tal operação.

Por parte da MULTICERT proceder-se-á à suspensão do certificado até ordem em contrário. No caso de o certificado ser suspenso devido a existirem fundadas razões para crer que o certificado foi emitido com base em informações erróneas ou falsas, que as informações nele contidas deixaram de ser conformes com a realidade ou que a confidencialidade da chave privada foi violada o processo poderá apenas terminar com a revogação incondicional do certificado.

5.4.8 Limites do Período de Suspensão

Um certificado pode ser suspenso por tempo indefinido. No entanto esta suspensão nunca deve ultrapassar a data da sua expiração.

5.4.9 Frequência de Emissão de CRLs (se aplicável)

As CRLs da MULTICERT CA serão emitidas periodicamente pela MULTICERT, mesmo que não existam alterações a ser reportadas, de forma a assegurar a continuidade da informação no tempo. Cada CRL tem uma duração que é dada por dois campos de dados: "data de emissão" e "data de próxima emissão". Cada CRL será emitida antes da "data de próxima emissão" da CRL anterior.

A MULTICERT publicará as CRLs de acordo com os requisitos legais.

5.4.10 Requisitos para Verificação de CRLs

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

Dependendo da importância de cada certificado, poderão vir a ser emitidas CRL's de emergência num prazo de 24 horas após ser recebido um pedido de revogação devidamente autorizado. As Partes Confiantes que estejam offline não se aperceberão deste facto e apenas recolherão a nova CRL na sua data de re-emissão programada. Sendo assim o método recomendado de obter a informação mais recente será fazendo o pedido online através de um servidor de informação de estado da MULTICERT CA, que seja notificado das CRLs de emergência.

5.4.11 Outras Formas de Anúncio de Revogação

No caso de ser emitida uma CRL de emergência pela MULTICERT CA, prontamente informará todas as ER dentro da infra-estrutura MULTICERT, de forma oral ou electrónica, que um certificado foi revogado e que uma CRL de emergência foi emitida e está disponível.

5.5 Mudança de Chaves

O certificado da MULTICERT CA foi gerado e assinado pela MULTICERT ROOT CA, sendo esta responsável pela geração e assinatura do(s) novo(s) certificado(s) da MULTICERT CA aquando de uma mudança de chaves.

A MULTICERT CA não emitirá certificados cujos tempos de vida ultrapassem a data de expiração dos seus próprios certificados.

Todas as Entidades de Registo reconhecidas pela MULTICERT CA serão notificadas (oralmente ou por meios electrónicos) antes da actualização da chave da MULTICERT CA. Será da inteira responsabilidade das ER a notificação de toda a estrutura directamente abaixo de si, até aos titulares dos certificados digitais.

6 Controlos de Segurança da PKI

6.1 Controlos de Acesso Físico

Os sistemas da Autoridade de Certificação MULTICERT estão alojados num Centro de Dados que respeita os mais rigorosos padrões de segurança física.

Para garantir esses níveis de segurança, são cumpridas todas as normas, dando particular atenção aos aspectos seguintes:

- Vigilância manual e electrónica do Centro de Dados, 24 horas por dia, para garantir uma protecção adequada contra a possibilidade de intrusão.

- Restrição de acesso físico à sala onde se encontram os sistemas da Entidade de Certificação, ao pessoal autorizado.

- Acesso físico de pessoal não autorizado à sala onde se encontram os sistemas só poderá ser realizada mediante autorização especial e sempre acompanhados de uma pessoa autorizada.

- Manutenção de um *log* de acessos permanentemente actualizado e sujeito a uma auditoria periódica.

- Classificação e Marcação de toda a informação, qualquer que seja o suporte ou meio físico em que a mesma se encontre.

- Destruição ou Inibição de todos os suportes onde tenham estado armazenadas informações relacionadas à operação da Autoridade de Certificação e que estejam danificados ou que não sejam mais utilizados.

6.2 Controlo de acesso aos sistemas das Entidades de Registo

As Entidades de Registo, enquanto locais de acesso público devem possuir Controlos de acesso ao nível dos sistemas que estão directamente ligados à Entidade de Certificação e ao nível do hardware e software que compõe o seu sistema de operação.

Salientam-se como pontos determinantes que deverão ser assegurados pela Entidade de Registo:

- A protecção da chave privada da Entidade de Registo deverá ser assegurada através do suporte de *hardware* criptográfico;
- Todas as operações que obriguem à utilização da chave privada deverão estar controladas através de um *PIN* ou de uma *password* de acesso (se possível de tipo dinâmico);
- A chave privada nunca deverá existir em claro, devendo estar cifrada por uma chave/segredo partilhada por uma ou mais pessoas da Autoridade de Registo.

Deve ser efectuado um controlo de acessos físico ao local onde se encontram as máquinas que comunicam com a Entidade de Certificação.

6.3 Controlos Ambiental das Instalações

Para garantir uma adequada protecção contra contingências ambientais as instalações onde se encontram alojados, os sistemas da Entidade de Certificação MULTICERT, estão providas de mecanismos adequados de prevenção e protecção.

De entre os mecanismos contemplados salientam-se:

- A existência de circuitos alternativos e UPS's para garantir que os sistemas da Entidade de Certificação ficarão disponíveis mesmo em caso de falha do fornecimento de energia eléctrica;

- Suporte de energia alternativo para os equipamentos de condicionamento atmosférico;

- Manutenção dos sistemas da Entidade de Certificação num ambiente controlado isolado de elementos ambientais vários, como sejam, a água, as variações de temperatura, a humidade e ainda de magnetismos vários.

- Existência de sistemas de detecção e combate automático a incêndios na zona de segurança onde residem os equipamentos.

6.4 Plano de Continuidade do Negócio

A Entidade de Certificação MULTICERT possui o seu próprio Plano de Continuidade do Negócio que inclui um conjunto de procedimentos de excepção, com vista à manutenção das operações em caso de acidente, atentado ou catástrofe natural. Uma das peças mais importantes deste Plano consiste na manutenção de uma réplica de toda a informação crítica num *site* de recuperação com um nível de segurança semelhante.

6.5 Controlos de Segurança Procedimentais

6.5.1 Segregação de Funções na Operação da Entidade Certificadora

Com vista à manutenção de níveis adequados de segurança na operação da Entidade de Certificação, estão definidas três funções distintas, no contexto da operação dos sistemas da Entidade de certificação MULTICERT.

- Master User – será o responsável pela configuração e gestão dos sistemas da Entidade de Certificação, quer ao nível do *hardware* quer ao nível do *software*. Será a única função que terá acesso directo à máquina e ao código do produto que suporta o sistema da Entidade de Certificação;

- Officer – Responsável pela gestão e manutenção das políticas de certificação e do CPS, pela gestão do pessoal e pela manutenção dos procedimentos de operação. Paralelamente

procederá ao controle e auditoria das operações realizadas pelos *Administrators*, na sua operação diária;

- Administrator – responsável pela operação diária da Entidade de Certificação, nomeadamente a emissão, revogação e renovação de certificados, bem como de todos os processos operacionais de relacionamento com as Entidades de registo e os clientes finais.

6.5.2 Segregação de Funções na Operação da Entidade de Registo

Ao nível das Entidades de Registo, embora se aconselhe a criação de uma estrutura de dois níveis de responsabilidade - o administrador e os operadores -, onde apenas o administrador possa assinar mensagens com a chave privada da Entidade de Registo, admite-se a possibilidade de que ambos os níveis sejam desempenhados por uma única pessoa.

Estas pessoas serão os responsáveis por:

- aceitar subscrições e pedidos dos clientes (para emissão, alteração ou revogação dos certificados);
- verificar os formulários de adesão/alteração/cessação de serviço e proceder à respectiva aceitação;
- assegurar a transmissão segura de todos os dados à entidade de certificação;
- fornecer ao utilizador os códigos de autorização para a obtenção de certificados *on-line*.

6.5.3 Identificação e Autorizações de cada Função

Todos os elementos da Entidade de Certificação MULTICERT que necessitem de operar directamente com os sistemas devem:

- Ter o seu nome e a sua função incluída na lista de acessos às instalações onde residem os sistemas da Entidade de Certificação.

- Ter o seu nome e a sua função incluída na lista de acessos aos sistemas da Entidade de Certificação.

- Obter um certificado especial emitido pela Entidade de Certificação MULTICERT, que será armazenado num *smart card* ou *token* e protegido por um PIN, para que possa ser identificado e devidamente autorizado a interagir com o sistema de controle e operação da Entidade de Certificação.

- Possuir credenciais de acesso ao *software* que controla e gere a infra-estrutura de chaves públicas (dentro dos limites específicos da função que desempenha).

Refira-se ainda que todos os certificados e credenciais concedidas aos funcionários identificados são pessoais e intransmissíveis, verificadas por sistemas de controle específicos e mecanismos de autorização

6.5.4 Requisitos Procedimentais para Operações Especiais

O procedimento de geração de uma nova chave privada para a Entidade de Certificação exige a presença de mais de duas pessoas autorizadas para o efeito, devendo, sempre que possível, incluir-se neste grupo pelo menos um representante da entidade credenciadora e de um auditor avalizado.

Em particular, no caso da geração de uma nova chave privada da Entidade de Certificação, seja por necessidade de revogação da chave seja por renovação, o processo deve utilizar hardware criptográfico de geração de chaves pelo menos nível FIPS-140 nível 2 e permitir que o segredo que protege a chave privada ou a própria chave privada seja dividida pelo número de pessoas presentes na cerimónia.

Após a divisão dos segredos, cada parte deve ser guardada num envelope fechado, selado e guardado em locais seguros diferentes. É essencial que a reconstrução da chave ou do segredo que protege a chave seja apenas efectuada pela presença simultânea das pessoas (ou seus legítimos representantes) que estiveram presentes na altura da criação da chave da Entidade de Certificação.

A divisão da chave pretende excluir a hipótese de existir uma só pessoa que possa reconstituir a chave privada da Entidade de Certificação. Além disso, traz mais confiança ao sistema na exigência por parte do CPS da presença física de mais do que uma pessoa.

Quaisquer outros procedimentos especiais que venham a ser identificados nesta secção do documento devem ter o envolvimento simultâneo de pelo menos duas pessoas devidamente autorizadas para o efeito.

6.6 Controlos de Segurança do Pessoal

6.6.1 Requisitos de Admissão e de Operação dos Funcionários da Entidade de Certificação

Todos os funcionários da entidade de certificação cumprem um conjunto de critérios fundamentais para que possam estar ao serviço da MULTICERT, nomeadamente:

- Foram objecto de uma identificação positiva.
- Estão contratualmente ligados à MULTICERT para o desempenho de uma função específica, e cujas responsabilidades estão devidamente expressas no contrato de trabalho.
- Assinaram um documento específico relativamente à manutenção de absoluta confidencialidade sobre os dados recolhidos durante o processo de certificação.
- Foi-lhes atribuído uma das três funções de operação dos sistemas da entidade de certificação (sempre que de tal necessitem para o desempenho da sua função específica).
- Receberam formação adequada, em particular sobre os procedimentos de segurança da Entidade de certificação e das Entidades de registo, sobre a utilização do *software* da PKI (se aplicável), sobre as permissões que estão subjacentes à sua função específica na operação dessa infra-estrutura e sobre o Plano de Continuidade de Negócio que está em

vigor.

- Recebem periodicamente uma reciclagem sobre os temas mencionados no ponto anterior.

- Estão sujeito a sanções financeiras e laborais graves em caso de abuso de confiança e/ou realização de acções não autorizadas.

- São possuidores de cópias autenticadas dos manuais de procedimentos da Entidade de certificação, em relação aos quais recebem notificações de actualização num período máximo de dois dias após a sua efectivação.

6.6.2 Requisitos de Acesso de Funcionários Externos à Entidade de Certificação

Todos os acessos de elementos externos à organização MULTICERT às suas instalações ou sistemas respeitam um conjunto de condições definidas contratualmente entre as duas entidades, entre as quais se destacam:

- A existência de uma identificação presencial positiva do visitante antes que possa aceder às instalações da Entidade de certificação;

- A existência de um contrato ou acordo de colaboração no qual estejam perfeitamente definidos os propósitos da colaboração, as permissões necessárias de acesso às instalações ou sistemas e as sanções em que incorre o visitante e a organização a que pertence em caso de abuso de confiança e/ou realização de acções não autorizadas;

- Todo e qualquer acesso (e permanência) à sala onde se encontram os sistemas da Entidade de certificação só poderá ser realizado na companhia de pelo menos um elemento da organização MULTICERT;

- Qualquer contacto de um elemento externo com os sistemas da Entidade de certificação (nomeadamente para funções de auditoria ou manutenção) deverá ser, se possível, realizado por intermédio de um funcionário da MULTICERT que o acompanhe; quando tal não for possível, deve ser criado um perfil específico com permissões mínimas de acesso ao sistema para garantir a realização das operações que estejam na base desta interacção.

7 Controlos de Segurança Técnicos

7.1 Geração do Par de Chaves

Todas as chaves privadas da MULTICERT são geradas num *hardware criptográfico* preparado para o efeito de acordo com as normas de segurança FIPS 140-1 (no mínimo de nível 2).

O método (algoritmo) usado para gerar pares de números primos para criar o módulo deve criar primos da dimensão adequada, que esteja de acorde com os requerimentos habituais para primos RSA.

O método usado para gerar os primos deve admitir um número suficientemente largo de primos diferentes (pelo menos, maior que 2^{100}), e esses primos devem ser gerados com igual (ou quase igual) probabilidade de selecção, em particular deve dar-se o caso de nenhum primo ter uma probabilidade de ser gerado maior que 2^{-100}.

O método usado para implementar a geração de primos deve ser seguro contra falhas. Isto é, no caso de qualquer tipo de falha no sistema, não deve ser possível que os primos que não estejam de acordo com estes requisitos sejam gerados.

O Hardware Criptográfico usado pela Multicert deve ser capaz de gerar chaves RSA de pelo menos 2048 bits de tamanho.

7.2 Controlos de Segurança sobre os Dados de Activação

Os dados de activação utilizados para emissão de certificados, são gerados automaticamente sem intervenção humana através de software/hardware da Autoridade de Certificação, estando o seu envio para o subscritor também automatizado, através de gateways com sistemas de envio automáticos e nos quais não é necessária a intervenção humana. Estes dados são necessários para a recolha do certificado pelo subscritor, pelo que será guardado em disco uma hash de cada um destes dados. Após a recolha do certificado pelo subscritor, será inibida a reutilização dos dados.

No mínimo serão geradas duas chaves de activação, sendo cada uma enviada por meio e/ou destino distinto para o subscritor, e sendo constituída por um mínimo de 16 caracteres alfanuméricos. Na sua geração serão utilizados algoritmos que garantam um grau de aleatoriadade adequado.

7.3 Controlos de Segurança do Sistema Central da Entidade de Certificação

7.3.1 Controlos de Segurança Básicos

Para garantir os adequados níveis de segurança sobre o sistema lógico onde reside o *software* da entidade de certificação MULTICERT, cada instância deste sistema deverá oferecer as

seguintes garantias:

- Controle de acessos aos diversos serviços e perfis da infra-estrutura de chaves públicas.
- Segregação de funções na interacção com o sistema.
- Definição clara das autorizações de cada utilizador através de um sistema de perfis gerido pela própria aplicação.
- Utilização de serviços criptográficos para protecção das comunicações e da base de dados.
- Arquivo automático dos registos de auditoria do sistema, tanto em relação aos dados da Entidade de Certificação como em relação aos dados dos utilizadores finais.
- Auditoria assegurada para todos os eventos relevantes.
- Mecanismos de recuperação automática das chaves utilizadas.

7.3.2 Controlos de Segurança Operacional

Para garantir a consistência do ambiente de operação da Entidade de Certificação, estão implementados controlos de segurança para a gestão das configurações dos ambientes operativos.

Assim sendo, todos os desenvolvimentos/instalações de *software* utilizados para a operação e manutenção da Entidade de Certificação são previamente testados e validados em ambientes de teste e/ou certificados por uma terceira parte de confiança.

7.4 Controlos de Segurança de Rede no Acesso ao Sistema Central da Autoridade de Certificação

O sistema central da Entidade de Certificação só poderá ser acedido remotamente a partir de máquinas previamente autorizadas por um administrador do sistema. Do mesmo modo, apenas comandos *standard* devidamente catalogados como comandos de operação da Entidade de Certificação serão aceites pela mesma.

7.5 Controlos de Segurança dos Módulos Criptográficos

Os módulos criptográficos utilizados pela Entidade de Certificação estão conforme a norma FIPS 140-1 de nível 3. Os módulos criptográficos utilizados pelas Entidades de registo seguem a norma FIPS 140-1 de nível 2.

8 Perfis dos Certificados e das CRLs

8.1 Perfil do Certificado

8.1.1 Número da Versão

A MULTICERT CA vai emitir certificados com o número de versão 2 (dois), que corresponde a certificados X.509 v3.

8.1.2 Extensões do Certificado

- *AuthorityKeyIdentifier*: O mesmo que o SubjectKeyIdentifier do emissor (MULTICERT ROOT CA). (Não crítica).

- *SubjectKeyIdentifier*: O hash SHA-1 do módulo do valor da chave pública (Não crítica).

- *CRLDistributionPoints*: O *DistributionPoint* contém dois CDP's baseados em URI's:

Ldap://[MULTICERT-CADirectory server DNS-Name]/

cn= MULTICERT-CA-ι^{x},

o= MULTICERT-CA,

c=PT /?certificateRevocationList?base

http://[MULTICERT CA Web server DNS-Name]/CA/MULTICERT- CA -ι^{x}.crl

ι^{x} = Significa a instalação n.º x da MULTICERT-CA. ι^{x} é substituído por um número sequencialmente incrementado começando em 01

CRLIssuer é o *issuer name* do certificado da MULTICERT CA (Não crítica).

- Certificate Policies: A única política aplicável a este Certificado. (Não crítica).

PolicyIdentifier = [Identificados da *Policy*]

PolicyQualifierId = The CPS OID {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 2 1}

cPSuri =http://[MULTICERT CA Web server DNS-Name]/CPS/MULTICERT-CA-CPS.txt

- Restrições Básicas: cA = TRUE

pathLenConstraint = omitido (Crítica).

- *KeyUsage*: *KeyCertSign*, *cRLSign*, assume que a MULTICERT CA usa o mesmo par de chaves para emitir certificados de sub-CAs e CRLs (Crítica).

8.1.3 *Algorithm Object Identifiers* – OID's

Os certificados a emitir pela MULTICERT CA devem ser assinados usando o algoritmo RSA.

8.1.4 Formato dos Nomes

Distinguished Name da MULTICERT CA:

C=PT	(País)
O=MULTICERT- CA	(Organização)
CN=MULTICERT- CA- ι^x	(*Common Name*)

8.1.5 Identificador da *Certificate Policy*

O Object Identifier para a *Policy*.

8.1.6 Extensão crítica *Certificate Policy*

Um utilizador de um certificado emitido com a extensão *Certificate Policy* como crítica, e que contenha o OID da *Certificate Policy* em questão, tem de aceitar todos os termos e condições aí definidas. Mais ainda, caso o apontador para o CPS esteja presente nesse certificado, o utilizador deverá aceitar todos os termos e condições definidas no CPS.

8.2 Perfil das CRLs

8.2.1 Número da Versão

A MULTICERT CA vai suportar a versão 1 (um), que corresponde a CRLs X.509 CRL v2.

8.2.2 Extensões às CRLs

As CRLs emitidas pela MULTICERT CA vão conter as seguintes extensões:

- *AuthorityKeyIdentifier*: É o hash SHA-1 do módulo, do valor da chave pública. O mesmo que o SubjectKeyIdentifier no certificado do emissor (MULTICERT-CA) (não crítica).

- *CRLNumber*: Uma contagem sequencial de todas as CRLs emitidas (não crítica).

9 Administração de Especificações

9.1 Procedimento Para Mudança de Especificações

9.1.1 Procedimentos de Alteração do CPS

9.1.1.1 Lista de Alterações

Toda e qualquer alteração que venha a ser realizada ao CPS da Autoridade de certificação MULTICERT CA será objecto de um documento de proposta de alterações.

9.1.1.2 Mecanismo de Notificação

As alterações propostas a uma política serão colocadas na Internet e comunicadas às Entidades de Registo.

9.1.1.3 Comentários

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

9.1.1.4 Mecanismo para Tratar os Comentários

Uma vez compilados os comentários será apresentada uma proposta de alterações formal à MULTICERT, devidamente acompanhada dos comentários recolhidos. A MULTICERT CA terá como obrigação o pedido de um parecer à Autoridade Credenciadora sobre o impacto destas alterações na credenciação da Entidade de Certificação MULTICERT CA.

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

9.1.1.5 Período de Entrada em Efeito das Alterações

Após este processo ser concluído as alterações passarão à prática após 30 dias. Serão adoptados mecanismos de controlo para garantir que todas as alterações às CPs e ao CPS são rasteadas e que é adoptado um correcto mecanismo de controlo de versões.

9.2 Políticas de Publicação e Notificação

9.2.1 Requerimento de Publicação e Notificação

Todos os ítems constantes das CPs e do CPS da MULTICERT CA estão sujeitos a publicação e notificação.

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

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

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

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

9.2.2 Publicação do CPS Actualizado

O documento de CPS, devidamente actualizado deverá estar permanentemente disponível através do URL http://www.multicert.com/CPS/MULTICERT-CA-CPS.html .

9.3 Procedimento de Aprovação do CPS

Este CPS é aprovado pelos representantes legais da MULTICERT S.A., com poderes para tal e carece da sua aprovação para ser alterado.

Fim do Documento