Entidade de Certificação Raiz
de Cabo Verde

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA ENTIDADE DE CERTIFICAÇÃO RAIZ DE CABO VERDE (DPC DA ICP-CV)

Políticas

PJ.ECRCV_24.1.1_0001_pt.doc

Identificação do Projecto: ECRCV

Identificação da CA: ECR-CV

Nível de Acesso: Público

Versão: 1.0

Data:18/08/20102

Sumário

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA ENTIDADE DE CERTIFICAÇÃO RAIZ DE CABO VERDE (DPC DA ICP-CV)..... 1

Resumo Executivo..... 13

1. Introdução..... 14

1.1. Objectivos..... 14

1.2. Público-Alvo..... 14

1.3. Estrutura do Documento..... 14

2. Acrónimos e definições..... 15

2.1. Acrónimos..... 16

2.2. Definições..... 16

3. contexto Geral..... 19

3.1. Objectivo..... 20

3.2. Enquadramento..... 21

3.3. Identificação do documento..... 21

3.4. Participantes na Infra-Estrutura de Chave Pública..... 21

3.4.1. ECR-CV..... 21

3.4.2. EC..... 22

3.4.3. Entidades ou Unidades de Registo..... 22

3.4.4. Titulares de certificados..... 22

3.4.5. Patrocinador..... 22

3.4.6. Partes Confiantes..... 23

3.4.7. Outros participantes..... 23

3.4.7.1. Autoridade Credenciadora..... 23

3.4.7.2. Conselho Gestor..... 24

3.5. Utilização do Certificado..... 25

3.5.1. certificados emitidos..... 25

3.5.2. Utilização adequada..... 25

3.5.3. Utilização não autorizada 25
3.6. Gestão das Políticas 26
4. disposições Legais 26
4.1. Obrigações e Direitos 27
4.1.1. Obrigações da ECR-CV 27
4.1.2. Obrigações das unidades de registo 28
4.1.3. Obrigações dos titulares de certificados 28
4.1.4. Obrigações das partes confiantes 29
4.1.5. Obrigações do Repositório 29
4.2. Responsabilidades 30
4.2.1. Responsabilidades da ECR-CV 30
4.2.2. Responsabilidades da Unidade de Registo 31
4.3. Publicação e Repositório 31
4.3.1. Publicação de informação da ECR-CV 31
4.3.2. Frequência de Publicação 32
4.3.3. Controlo de acesso 32
4.4. Auditoria de Conformidade 32
4.4.1. Quem realiza Auditoria 32
4.4.2. Frequência ou motivo da auditoria 32
4.4.3. Identidade e qualificações do auditor 33
4.4.4. Relação entre a ECR-CV e o auditor externo 33
4.4.5. Âmbito da auditoria 34
4.4.6. auditoria com resultado deficiente 34
4.5. Sigilo 34
4.5.1. Chaves Privadas 34
4.5.2. Verficação Estado do Certificado 34
4.5.3. Quebra de sigilo por motivos legais 34
4.5.4. Informações a terceiros 34
4.5.5. Divulgação por solicitação do titular 35
4.5.6. Direitos de propriedade intelectual 35
5. Identificação e Autenticação 35

5.1. Registo Inicial 36
5.1.1. Disposições Legais 36
5.1.1.1. Tipos de nomes 36
5.1.1.2. Necessidade de nomes significativos 36
5.1.1.3. Interpretação de formato de nomes 36
5.1.1.4. Unicidade de nomes 36
5.1.1.5. Procedimento para resolver disputa de nomes 36
5.1.1.6. Reconhecimento, autenticação de marcas registadas 37
5.1.1.7. comprovação de posse de chave privada 37
5.1.1.8. Autenticação da identidade de um indivíduo 37
5.1.1.9. Autenticação da identidade de uma organização 37
5.1.1.10. Validação dos poderes de autoridade ou representação 38
5.2. Critérios para interoperabilidade 38
5.3. Identificação e Autenticação 38
5.3.1. renovação de certificados 38
5.3.2. renovação de chaves de rotina 39
5.3.3. renovação de chaves, após revogação 39
5.4. pedidos de revogação de chaves 39
6. Requisitos operacionais do ciclo de vida do certificado 40
6.1. Pedido de Certificado 41
6.1.1. Requisitos 41
6.1.2. Quem pode subscrever um pedido de certificado? 41
6.1.3. Processo de registo e responsabilidades 41
6.2. Processamento do pedido de certificado 41
6.2.1. Requisitos 41
6.2.2. Processo para a identificação e funções de autenticação 42
6.2.3. Aprovação ou recusa de pedidos de certificado 42
6.2.4. Prazo para processar o pedido de certificado 42
6.3. Emissão de Certificado 42
6.3.1. Procedimento para a emissão de certificado da ECR-CV 43
6.3.2. Procedimentos para a emissão de certificado de EC 43

6.4. Aceitação do Certificado 44
6.4.1. Procedimentos para a aceitação de certificado 44
6.4.2. Publicação do certificado 44
6.4.3. Notificação da emissão de certificado a outras entidades 45
6.5. Uso do certificado e par de chaves 45
6.5.1. Uso do certificado e da chave privada pelo titular 45
6.5.2. Uso do certificado e da chave pública pelas partes confiantes 45
6.6. Renovação de Certificados sem geração de novo par de chaves 45
6.7. Renovação de certificado com geração de novo par de chaves 46
6.7.1. Definição 46
6.7.2. Motivo para a renovação de certificado com geração de novo par de chaves 46
6.7.3. Quem pode solicitar uma nova chave pública 46
6.7.4. Processamento do pedido de renovação de certificado 46
6.7.5. Notificação da emissão de novo certificado ao titular 46
6.7.6. Procedimentos para aceitação de um novo certificado 46
6.7.7. Publicação de certificado após geração de novo par de chaves 46
6.7.8. Notificação da emissão de certificado renovado a outras entidades 47
6.8. Modificação de certificados 47
6.9. Suspensão e revogação de certificado 47
6.9.1. Âmbito 47
6.9.2. Circunstâncias para revogação 47
6.9.3. Quem pode submeter o pedido de revogação 48
6.9.4. Procedimento para o pedido de revogação 48
6.9.5. Produção de efeitos da revogação 49
6.9.6. Prazo para processar o pedido de revogação 49
6.9.7. Requisitos de verificação da revogação pelas partes confiantes 49
6.9.8. Circunstâncias para a suspensão 49
6.9.9. Quem pode solicitar suspensão 49
6.9.10. Procedimento para pedido de suspensão 49
6.9.11. Limite do período de suspensão 49
6.9.12. Frequência de emissão LCR 49

6.9.13. Período máximo entre a emissão e a publicação da LCR....50
6.9.14. Disponibilidade de verificação on-line do estado / revogação de certificado....50
6.9.15. Requisitos de verificação on-line de revogação....50
6.9.16. Outras formas disponíveis para divulgação de revogação....50
6.9.17. Requisitos em caso de comprometimento de chave privada....50
6.10. Serviços sobre o estado do certificado....50
6.10.1. Características operacionais....50
6.10.2. Disponibilidade do serviço....50
6.11. Fim de subscrição....50
6.12. Procedimentos de auditoria de segurança....51
6.12.1. Tipo de eventos registados....51
6.12.2. Frequência da auditoria de registos....51
6.12.3. Período de retenção dos registos de auditoria....51
6.12.4. Protecção dos registos de auditoria....51
6.12.5. Procedimentos, para a cópia de segurança dos registos....52
6.12.6. Sistema de recolha de registos (Interno / Externo)....52
6.12.7. Notificação de agentes causadores de eventos....52
6.12.8. Avaliação de vulnerabilidades....52
6.13. Arquivo de registos....52
6.13.1. Tipo de dados arquivados....52
6.13.2. Período de retenção em arquivo....52
6.13.3. Protecção dos arquivos....53
6.13.4. Procedimentos para as cópias de segurança do arquivo....53
6.13.5. Requisitos, para validação cronológica dos registos....53
6.13.6. Sistema de recolha de dados de arquivo (Interno / Externo)....53
6.13.7. Procedimentos de recuperação e verificação de informação arquivada....53
6.14. Renovação de chaves....53
6.15. Recuperação em caso de desastre ou comprometimento....54
6.15.1. Âmbito....54
6.15.2. Procedimentos em caso de incidente ou comprometimento....54
6.15.3. Corrupção dos recursos informáticos, do software e/ou dos dados....54

6.15.4. comprometimento da chave privada da entidade....54
6.15.5. Capacidade de continuidade da actividade em caso de desastre....55
6.16. Procedimentos em caso de extinção da ECR-CV....55
6.17. Retenção e recuperação de chaves (Key escrow)....55
6.17.1. Chave da ECR-CV....55
6.17.2. Políticas e práticas de recuperação de chaves....55
6.17.3. encapsulamento e recuperação de chaves de sessão....56
7. Medidas de segurança física, de gestão e operacionais....56
7.1. Resumo....56
7.2. Medidas de segurança física....57
7.2.1. Construção e Localização física das Instalações da EC....57
7.2.2. Acesso físico ao local....57
7.2.3. Energia e ar condicionado....58
7.2.4. Exposição à água....59
7.2.5. Prevenção e protecção contra incêndio....59
7.2.6. Salvaguarda de suportes de armazenamento....59
7.2.7. Eliminação de resíduos....60
7.3. Instalações externas (alternativa), para recuperação de segurança....60
7.4. Medida de segurança dos processos....60
7.5. Funções de Confiança....61
7.5.1. Pessoas Autenticadas....61
7.5.2. Grupo de Trabalho de Administração de Segurança....61
7.5.3. Grupo de Trabalho de Administração de Registo....62
7.5.4. Grupo de Trabalho de Administração de Sistemas....62
7.5.5. Grupo de Trabalho de Operação de Sistemas....62
7.5.6. Grupo de Trabalho de Auditoria de Sistemas....63
7.5.7. Conselho Executivo (consultor de Sistemas)....63
7.5.8. Grupo de Trabalho de Custódia....64
7.6. Número de pessoas exigidas por tarefa....64
7.7. Identificação e Autenticação, para cada função....64
7.8. Funções que requerem separação de responsabilidades....65

7.9. Medidas de segurança de pessoal 65
7.10. Requisitos de admissão 66
7.11. Procedimento de verificação de antecedentes 66
7.12. Requisitos de formação e treino 66
7.13. Frequência e requisitos para acções de reciclagem 66
7.14. Frequência e sequência da rotação de funções 67
7.15. Sanções para acções não autorizadas 67
7.16. Requisitos para contratação de pessoal 67
7.17. Documentação fornecida ao pessoal 67
8. Medidas de Segurança Técnica 67
8.1. Âmbito 67
8.2. Geração e instalação do par de chaves 69
8.2.1. Geração do par de chaves 69
8.2.2. Entrega da chave privada ao titular 69
8.2.3. Entrega da chave pública ao emissor do certificado 69
8.2.4. Entrega da chave pública da EC às partes confiantes 69
8.2.5. Dimensão das chaves 69
8.2.6. Parâmetros da chave pública e verificação da qualidade 70
8.2.7. Fins a que se destinam as chaves (campo "key usage" X.509 v3) 70
8.3. Protecção da chave privada e características do módulo criptográfico 70
8.4. Normas e medidas de segurança do módulo criptográfico 70
8.4.1. Segurança Física 70
8.4.2. Certificações Regulamentares 70
8.4.3. Autenticação 70
8.5. Controlo multi-pessoal (m de n) para a chave privada 71
8.6. Retenção da chave privada (Key escrow) 71
8.7. Cópia de segurança da chave privada 71
8.8. Arquivo da chave privada 71
8.9. Transferência da chave privada para/do módulo criptográfico 71
8.10. Armazenamento da chave privada no módulo criptográfico 72
8.11. Processo para activação da chave privada 72

8.12. Processo para desactivação da chave privada 72
8.13. Processo para destruição da chave privada 72
8.14. Avaliação/nível do módulo criptográfico 72
8.15. Outros aspectos da gestão do par de chaves 73
8.15.1. Arquivo da chave pública 73
8.15.2. Períodos de validade do certificado e das chaves 73
8.16. Dados de activação 73
8.16.1. Geração e instalação dos dados de activação 73
8.16.2. Protecção dos dados de activação 73
8.16.3. Outros aspectos dos dados de activação 73
8.17. Medidas de segurança informática 74
8.17.1. Requisitos técnicos específicos 74
8.17.2. Avaliação/nível de segurança 74
8.18. Ciclo de vida das medidas técnicas de segurança 74
8.18.1. Medidas de desenvolvimento do sistema 74
8.18.2. Medidas para a gestão da segurança 74
8.18.3. Ciclo de vida das medidas de segurança 75
8.19. Medidas de Segurança da rede 75
8.20. Validação cronológica (Time-stamping) 75
9. Perfis de Certificado, CRL e OCSP 75
9.1. Perfis de Certificado da ECR-CV 76
9.2. Número de versão 76
9.3. Restrições de nome 76
9.4. OID da DPC 77
9.5. Uso da extensão "Policy Constraints" 77
9.6. Sintaxe e semântica dos qualificadores de política 77
9.7. Semântica de processamento para as extensões críticas de PC 77
9.8. Extensões de certificado da ECR-CV 77
9.9. Extensões de certificado de EC subordinada 81
9.10. Perfil de LCR 84
9.11. Número(s) de versão 85

9.12. Extensões de LCR da ECR-CV 85
9.13. Perfil OCSP 88
10. Administração de Especificação 88
10.1. Procedimentos de mudança de especificação 89
10.2. Políticas de publicação e notificação 89
10.3. Procedimentos para Aprovação 89
10.4. Outras Situações e Assuntos Legais 89
10.4.1. Taxas 89
10.5. Responsabilidade financeira 89
10.5.1. Seguro 90
10.6. Confidencialidade da informação processada 90
10.6.1. Âmbito da confidencialidade da informação 90
10.6.2. Informação fora do âmbito da confidencialidade da informação 90
10.6.3. Responsabilidade de protecção da confidencialidade da informação 91
10.7. Privacidade dos dados pessoais 91
10.7.1. Medidas para garantia da privacidade 91
10.8. Renúncia de garantias 91
10.9. Indemnizações 91
10.10. Termo e cessação da actividade 91
10.10.1. Termo 91
10.10.2. Substituição e revogação da DPC 92
10.10.3. Consequências da cessação de actividade 92
10.11. Notificação individual e comunicação aos participantes 92
10.12. Alterações 92
10.12.1. Procedimento para alterações 93
10.12.2. Prazo e mecanismo de notificação 93
10.12.3. Motivos para mudança de OID 93
10.13. Disposições para resolução de conflitos 93
10.14. Legislação aplicável 94
10.15. Conformidade com a legislação em vigor 94
10.16. Providências várias 94

10.16.1. Acordo completo..... 94
10.16.2. Independência..... 94
10.16.3. Severidade..... 94
10.16.4. Execuções (taxas de advogados e desistência de direitos)..... 95
10.16.5. Força Maior..... 95
10.16.6. Outras providências..... 95
Referências Bibliográficas..... 96

Identificador do documento: PJ.ECRCV_24.1.1_0001_pt.doc

Palavras-chave: ECR-CV, Declaração de Práticas de Certificação

Tipologia documental: Políticas

Título: Declaração de Práticas de Certificação da EC Raiz de Cabo Verde

Língua original: Português

Língua de publicação: Português

Data: 18/08/2010

Versão actual: 1.0

Identificação da EC: ECR-CV

RESUMO EXECUTIVO

Decorrente da implementação de vários programas públicos 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 e do governo electrónico (*eGovernment*), foi aprovado a criação da ICP-CV (Infra-estrutura de Chaves Públicas de Cabo Verde). Esta infra-estrutura fornece uma hierarquia de confiança, estabelecendo uma estrutura de confiança electrónica que proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e a confidencialidade das transacções ou informação.

Para o efeito, a ICP-CV compreenderá uma ECR-CV (Entidade de Certificação Raiz de Cabo Verde), que, além de prestar serviços de certificação de topo na ICP-CV, executa e zela pela aplicação das políticas de certificados e directrizes aprovadas pelo CG da ICP-CV.

Compete ainda à ECR-CV prestar os serviços de certificação, no nível hierárquico imediatamente abaixo ao seu na cadeia de certificação, de acordo com a legislação e normas aplicáveis às entidades de certificação estabelecidas em Cabo Verde para a emissão de certificados digitais qualificados.

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

1. INTRODUÇÃO

1.1. OBJECTIVOS

1.1.1. O objectivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Certificação Raiz de Cabo Verde (ECR-CV) no suporte à sua actividade de certificação digital.

1.2. PÚBLICO-ALVO

1.2.1. Este documento deve ser lido por:

a) Recursos humanos ao serviço da ECR-CV;

b) Terceiras partes encarregues de auditar a ECR-CV;

c) Todo o público, em geral.

1.3. ESTRUTURA DO DOCUMENTO

1.3.1. Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF, no documento RFC 3647[1], de acordo também com a estrutura do documento 'REQUISITOS MINIMOS DE REDACÇÃO PARA DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO (DPC) NO ÂMBITO DA ICP-CV'.

1.3.2. O ponto 2 do documento apresenta um conjunto de acrónimos e definições úteis para a leitura do documento. Os oito pontos seguintes são dedicados a descrever os procedimentos e práticas mais importantes no âmbito da certificação digital da Entidade de Certificação Raiz de Cabo Verde. O décimo primeiro ponto descreve matérias legais.

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

2. ACRÓNIMOS E DEFINIÇÕES

2.1. ACRÓNIMOS

Acrónimo	
ANSI	*American National Standards Institute*
CA	*Certification Authority* (o mesmo que EC)
DL	Decreto-lei
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EC	Entidade de Certificação
ECR-CV	Entidade de Certificação Raiz de Cabo Verde
ICP-CV	Infra-estrutura de chaves públicas de Cabo Verde
LCR	Lista de Certificados Revogados
MAC	*Message Authentication Codes*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier* (Identificador de Objecto)
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infra-estrutura de Chave Pública)
SHA	*Secure Hash Algorithm*
SSCD	*Secure Signature-Creation Device*
URI	*Uniform Resource Identifier*

2.2. DEFINIÇÕES

Definição	

Assinatura digital, conforme disposto no DL-nº33/2007, de 24 de Setembro	Modalidade de assinatura electrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura.
Assinatura electrónica, conforme disposto no DL-nº33/2007, de 24 de Setembro	Dados sob forma electrónica anexos ou logicamente associados a uma mensagem de dados e que sirvam de método de autenticação.
Assinatura electrónica avançada, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Assinatura electrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura electrónica qualificada, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade credenciadora, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Entidade competente para a credenciação e fiscalização das Entidades de Certificação.
Certificado, conforme disposto no DL-	Documento electrónico que liga os dados de

nº33/2007, de 24 de Setembro	verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado, conforme disposto no DL-nº33/2007, de 24 de Setembro	Certificado que contém os elementos referidos no artigo 67.º do DL 33/2007 [6] e é emitido por entidade de certificação que reúne os requisitos definidos no artigo 45.º do DL 33/2007.
Chave privada, conforme disposto no DL-nº33/2007, de 24 de Setembro	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento electrónico, ou se decifra um documento electrónico previamente cifrado com a correspondente chave pública.
Chave pública, conforme disposto no DL-nº33/2007, de 24 de Setembro	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves.
Credenciação, conforme disposto no DL-nº33/2007, de 24 de Setembro	Acto pelo qual é reconhecido a uma entidade, que o solicite e que exerça a actividade de entidade de certificação, o preenchimento dos requisitos definidos n**o DL-nº33/2007, de 24 de Setembro** para os efeitos nele, previstos.
Dados de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Um conjunto único de dados, como códigos ou chaves criptográficas privadas, usado pelo signatário para a criação de uma assinatura electrónica.
Dados de verificação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Um conjunto de dados, como códigos ou chaves criptográficas públicas, usado para verificar a assinatura electrónica.
Dispositivo de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de Setembro	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que,

	i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento electrónico, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Documento elaborado mediante processamento electrónico de dados.
Endereço electrónico, conforme disposto no DL-nº33/2007, de 24 de Setembro.	Identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos.

3. CONTEXTO GERAL

3.1. OBJECTIVO

3.1.1. O presente documento é uma DPC, cujo objectivo se prende com a definição de um conjunto de práticas para a emissão e validação de certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações mas antes informar, pelo que se pretende que este documento seja simples, directo e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

3.1.2. Este documento descreve as práticas gerais de emissão e gestão de certificados, seguidas pela ECR-CV, 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 ECR-CV.

3.1.3. Este documento pode sofrer actualizações regulares.

3.1.4. Os certificados emitidos pela ECR-CV contêm uma referência à presente 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.

3.2. ENQUADRAMENTO

3.2.1. As práticas de criação, assinatura e de emissão de Certificados, assim como de revogação de certificados inválidos levadas a cabo por uma EC são fundamentais para garantir a fiabilidade e confiança de uma ICP.

3.2.2. O presente documento aplica-se especificamente à ECR-CV, de acordo com a estrutura em uso no âmbito da ICP-CV e com os seguintes standards:

a) RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework;

b) RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile.

3.2.3. O presente documento especifica, respectivamente, como implementar os procedimentos e controlos usados na ECR-CV, e como a ECR-CV deve atingir os requisitos especificados nas normas da ICP-CV.

3.3. IDENTIFICAÇÃO DO DOCUMENTO

3.3.1. Este documento é uma DPC que é representada num certificado através de um número único designado de "identificador de objecto" (OID), sendo o valor do OID associado a este documento o 2.16.132.1.3.1.

3.3.2. Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	2.16.132.1.3.1.1
Data de Emissão	---
Validade	Não aplicável
Localização	http://pki.ecrcv.cv/pub/pol/ec_raiz_dpc_001_pt.html

3.4. PARTICIPANTES NA INFRA-ESTRUTURA DE CHAVE PÚBLICA

3.4.1. ECR-CV

a) A ECR-CV insere-se na hierarquia de confiança da ICP-CV, constituindo-se numa entidade de certificação de primeiro nível estabelecendo a raiz da cadeia de confiança da ICP-CV. Deste modo, a ECR-CV apenas emite certificados para assinar os certificados das ECs de nível hierárquico imediatamente inferior.

b) A ECR-CV emite:

c) O seu certificado auto-assinado;

d) O certificado das ECs;

e) A sua LCR.

3.4.2. EC

a) As ECs encontram-se no nível hierárquico imediatamente abaixo da ECR-CV e podem emitir certificados para os seguintes destinatários:

b) ECs Subordinadas;

c) Titulares de Certificado;

d) Equipamento tecnológico.

3.4.3. ENTIDADES OU UNIDADES DE REGISTO

a) Entidades ou Unidades de Registo são entidades às quais as ECs delegam a prestação de serviços de identificação, registo de utilizadores de certificados, bem como a gestão de pedidos de renovação e revogação de certificados.

b) As actividades de identificação e de registo das ECs são realizadas durante o processo de credenciação, não havendo entidades ou unidades de registo no âmbito de operação da ECR-CV.

3.4.4. TITULARES DE CERTIFICADOS

a) No âmbito deste documento, dado que se trata da DPC da ECR-CV, os titulares dos certificados serão as pessoas colectivas, desde que sob responsabilidade humana, o qual aceita o certificado e é responsável pela sua correcta utilização e salvaguarda da sua chave privada. Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um dos seus representantes legais.

b) O titular do certificado da ECR-CV (certificado- Auto assinado) é a ANAC.

c) Os titulares das ECs, que têm certificado assinado pela ECR-CV, são as próprias entidades responsáveis por elas, ou um representante legal nomeado para o efeito.

3.4.5. PATROCINADOR

Nada a assinalar.

3.4.6. PARTES CONFIANTES

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

b) Nesta DPC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido na hierarquia de confiança da ICP-CV, podendo ser ou não ser titular de certificados da comunidade ICP-CV.

3.4.7. OUTROS PARTICIPANTES

3.4.7.1. AUTORIDADE CREDENCIADORA

3.4.7.1.1. A Autoridade Credenciadora assume o papel de entidade que disponibiliza serviços de auditoria/inspecção de conformidade, no sentido de aferir se os processos utilizados pelas ECs nas suas actividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos na legislação e nomas vigentes.

3.4.7.1.2. Assim, consideram-se como principais atribuições as seguintes:

a) Acreditar as entidades de certificação;

b) Controlar as entidades de certificação;

c) Cobrar taxas pelos serviços de acreditação;

d) Zelar por que as entidades de certificação respondam pelo prejuízo causado a toda entidade ou pessoa física ou jurídica que se fie e razoavelmente nos certificados;

e) Auditar as entidades de certificação;

f) Zelar por que os dispositivos de segurança de criação de assinaturas electrónicas sejam conformes às condições previstas no artigo 28º do Decreto-lei 33/2007, de 24 de Setembro;

g) Celebrar acordos reconhecimento mútuo com autoridades de credenciação de países estrangeiros, desde que previamente autorizada pelo departamento governamental responsável pelas comunicações;

h) Manter informações na internet sobre a lista de entidades de certificação, e a suspensão e revogação de certificados digitais, bem como sobre os demais aspectos relevantes da certificação;

i) Definir os requisitos técnicos que qualifiquem a idoneidade de actividades desenvolvidas pelas entidades de certificação;

j) Avaliar as actividades desenvolvidas pelas entidades de certificação autorizadas conforme os requisitos técnicos definidos nos termos da alínea anterior;

k) Zelar pelo adequado funcionamento e eficiente prestação de serviço por parte de entidades de certificação em conformidade com as disposições legais e regulamentares da actividade;

l) O mais que lhe for cometido por lei.

3.4.7.2. CONSELHO GESTOR

O CG é responsável pela gestão global e administração da ICP-CV, competindo-lhe:

a) Definir e aprovar, de acordo com as normas ou especificações internacionalmente reconhecidas, as políticas e as práticas de certificação a observar pelas ECs que integram a ICP-CV;

b) Garantir que as declarações de práticas de certificação das várias ECs, incluindo a ECR-CV, estão em conformidade com as políticas de certificado da ICP-CV;

c) Definir e publicar os critérios para aprovação das entidades de certificação que pretendam integrar a ICP-CV;

d) Aprovar a integração na ICP-CV das ECs que obedeçam aos requisitos estabelecidos no presente diploma e que se enquadrem nos critérios previamente estabelecidos e referidos na alínea anterior;

e) Obter da Autoridade Credenciadora um parecer de auditoria e conformidade sobre as ECs que pretendam integrar a ICP-CV;

f) Aferir da conformidade dos procedimentos seguidos pelas ECs com as políticas e directivas aprovadas, sem prejuízo das competências legalmente cometidas à Autoridade Credenciadora;

g) Decidir pela exclusão de ECs da ICP-CV, em caso de não conformidade com as políticas e práticas aprovadas, comunicando tal facto à Autoridade Credenciadora;

h) Pronunciar-se sobre as melhores práticas internacionais no exercício das actividades de certificação e propor a sua aplicação.

3.5. UTILIZAÇÃO DO CERTIFICADO

3.5.1. CERTIFICADOS EMITIDOS

3.5.1.1. Os certificados emitidos pela ECR-CV são utilizados com o objectivo de:

a) Identificar a ECR-CV e as ECs;

b) Divulgar as chaves públicas da ECR-CV; e

c) Conferir credibilidade aos certificados das ECs integrantes da ICP-CV.

3.5.1.2. A emissão dos certificados é efectuada com o recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a ECR-CV e ICP-CV proporcionam. 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.

3.5.2. UTILIZAÇÃO ADEQUADA

3.5.2.1. Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela ECR-CV.

3.5.2.2. Os certificados emitidos pela ECR-CV são também utilizados pelas partes confiantes para verificação da cadeia de confiança de um certificado emitido sob a ICP-CV, 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 assinado pela ECR-CV.

3.5.2.3. Os certificados emitidos pela ECR-CV devem ser utilizados de acordo com a função e finalidade estabelecida neste documento e nas correspondentes Políticas de Certificados e de acordo com a legislação em vigor.

3.5.3. UTILIZAÇÃO NÃO AUTORIZADA

3.5.3.1. Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pelas regras da ICP-CV e pela legislação aplicável.

3.5.3.2. Os certificados emitidos pela ECR-CV não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

3.5.3.3. Os serviços de certificação oferecidos pela ECR-CV, não foram desenhados nem está autorizada a sua utilização em actividades de alto risco ou que requeiram uma actividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra actividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

3.6. GESTÃO DAS POLÍTICAS

A gestão desta DPC é da responsabilidade da ECR-CV, que pode ser contactada pelos telefones e no seguinte endereço:

Nome:	ANAC
Morada:	ANAC - CHÃ DE AREIA, PRAIA, CABO VERDE
Correio electrónico:	ecrcv@anac.cv
Fax:	2613069
Telefone:	260 44 00/01/02/03

4. DISPOSIÇÕES LEGAIS

4.1. OBRIGAÇÕES E DIREITOS

4.1.1. OBRIGAÇÕES DA ECR-CV

4.1.1.1. A ECR-CV está obrigada a:

a) Realizar as suas operações de acordo com esta DPC e com a sua Politica de Segurança;

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

c) Assegurar que as demais entidades envolvidas, nomeadamente Entidades de Certificação, tenham conhecimento dos seus direitos e obrigações;

d) Gerir a suas chaves privadas;

e) Proteger as suas chaves privadas;

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

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

h) Emitir certificados para Entidades de Certificação, públicas ou privadas;

4.1.1.2. A ECVR-CV deve notificar os subscritores dos seus certificados quando ocorrer:

a) Suspeita de comprometimento da sua chave;

b) Emissão de um novo par de chaves e do certificado correspondente;

c) Encerramento das actividades;

4.1.1.3. Ainda a ECR-CV, está obrigada a:

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

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

c) Arquivar sem alteração os certificados emitidos;

d) Garantir que pode ser determinada com precisão a data e hora em que se emitiu, revogou ou suspendeu um certificado;

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

f) Revogar os certificados nos termos do secção 6.9 deste documento e publicar os certificados revogados na LCR do seu repositório, com a frequência estipulada no ponto 6.9.12;

g) Publicar a sua DPC e no seu repositório garantindo o acesso às versões actuais assim como as versões anteriores;

h) Notificar com a rapidez necessária, em caso de proceder à revogação ou suspensão dos certificados emitidos, indicando o motivo que originou esta acção;

i) Identificar e registar todas as acções executadas, conforme as normas, práticas e regras estabelecidas pela Autoridade Credenciadora – Manter a conformidade dos seus processos, procedimentos e actividades com as normas, práticas e regras da ICP-CV e com a legislação em vigor;

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

k) Operar de acordo com a legislação aplicável;

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

m) Garantir a disponibilidade da sua LCR;

n) Em caso de cessar a sua actividade, comunicar o facto com uma antecedência mínima de três meses a todos os responsáveis dos certificados emitidos para as Entidades de Certificação subordinadas;

o) Cumprir com as especificações contidas na norma sobre Protecção de Dados Pessoais;

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

4.1.2. OBRIGAÇÕES DAS UNIDADES DE REGISTO

Nada a assinalar.

4.1.3. OBRIGAÇÕES DOS TITULARES DE CERTIFICADOS

É obrigação dos titulares dos certificados emitidos:

a) Tomar conhecimento dos direitos e obrigações, contemplados pela DPC e outros documentos conforme disposição das normas da ICP-CV;

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

c) Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita de comprometimento da chave privada correspondente à chave pública contida no certificado, de acordo com a secção 6.9;

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

e) Fornecer de modo completo e preciso todas as informações necessárias para a sua identificação. Devem informar a ECR-CV de qualquer modificação desta informação; e

f) Não monitorizar, manipular ou efectuar acções de "engenharia inversa" sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da ECR-CV.

4.1.4. OBRIGAÇÕES DAS PARTES CONFIANTES

É obrigação das partes que confiam nos certificados emitidos pela ECR-CV:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso no presente documento;

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

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

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

e) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando os meios que a ECR-CV publique no seu sítio Web.

4.1.5. OBRIGAÇÕES DO REPOSITÓRIO

4.1.5.1. A ANAC é responsável pelas funções de repositório da ECR-CV, publicando, entre outras, informação relativa às práticas adoptadas e à sua LCR.

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

a) Disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efectuadas em horário de menor utilização, garantindo-se durante o tempo da disponibilidade:

i. Mínimo de 99,990% de respostas a pedidos de obtenção da LCR;

ii. Mínimo de 99,990% de respostas a pedidos do documento da DPC;

4.1.5.3. Número máximo de pedidos de LCR: 50 pedidos/minuto;

4.1.5.4. Número máximo de pedidos da DPC: 50 pedidos/minuto;

4.1.5.5. Número médio de pedidos de LCR: 20 pedidos/minuto;

4.1.5.6. Número médio de pedidos da DPC: 20 pedidos/minuto.

4.1.5.7. O acesso à informação disponibilizada pelo repositório é efectuado através dos protocolos HTTPS e HTTP, estando implementados os seguintes mecanismos de segurança:

a) LCR e DPC só podem ser alterados através de processos e procedimentos bem definidos;

b) Plataforma tecnológica do repositório encontra-se devidamente protegida pelas técnicas mais actuais de segurança física e lógica;

c) Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

4.2. RESPONSABILIDADES

4.2.1. RESPONSABILIDADES DA ECR-CV

4.2.1.1. A ECR-CV responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua actividade de acordo com o art. 62º do Decreto-Lei nº 33/2007;

4.2.1.2. A ECR-CV 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 emitido por ela, uma vez que tenha conhecimento dele;

4.2.1.3. A ECR-CV assume toda a responsabilidade mediante terceiros pela actuação dos titulares das funções necessárias à prestação de serviços de certificação;

4.2.1.4. A responsabilidade da administração / gestão da ECR-CV assenta sobre bases objectivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;

4.2.1.5. A ECR-CV só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara e reconhecida por terceiros o limite quanto ao possível uso;

4.2.1.6. A ECR-CV 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;

4.2.1.7. A ECR-CV não responde se o destinatário dos documentos assinados electronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações; e

4.2.1.8. A ECR-CV não assume qualquer responsabilidade no caso de perda ou prejuízo:

4.2.1.9. Dos serviços que presta, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;

4.2.1.10. Ocasionado pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmos nas normas da ICP-CV;

4.2.1.11. Ocasionado pelo uso indevido ou fraudulento dos certificados ou LCR emitidos pela ECR-CV.

4.2.2. RESPONSABILIDADES DA UNIDADE DE REGISTO

Nada a assinalar.

4.3. PUBLICAÇÃO E REPOSITÓRIO

4.3.1. PUBLICAÇÃO DE INFORMAÇÃO DA ECR-CV

4.3.1.1. A ECR-CV mantém um repositório em ambiente Web, permitindo que as Partes Confiantes efectuem pesquisas on-line relativas à revogação e outra informação referente ao estado dos Certificados.

4.3.1.2. A ECR-CV disponibiliza sempre a seguinte informação pública on-line:

4.3.1.3. Cópia electrónica actualizada desta DPC:

a) DPC da ECR-CV disponibilizada em Língua Portuguesa no URI:

b) http://pki.ecrcv.cv/pub/pol/ec_raiz_dpc_001_pt.html

c) DPC da ECR-CV disponibilizada em Língua Inglesa no URI: http://pki.ecrcv.cv/pub/pol/ec_raiz_dpc_001_en.html

4.3.1.4. LCR da ECR-CV - URI: http://pki.ecrcv.cv/pub/crl/ec_raiz_crl001.crl;

4.3.1.5. Certificado da ECR-CV – URI: http://pki.ecrcv.cv/pub/cert/ec_raiz_ 001.crt;

4.3.1.6. Outra informação relevante – URI: http://pki.ecrcv.cv/pub/info/.

4.3.1.7. Adicionalmente serão conservadas todas as versões anteriores das DPC's da ECR-CV, disponibilizando-as a quem as solicite (desde que justificado), ficando, no entanto fora do repositório público de acesso livre.

4.3.2. FREQUÊNCIA DE PUBLICAÇÃO

4.3.2.1. A ECR-CV garante que será disponibilizada sempre a seguinte informação pública on-line, utilizando os mesmos protocolos e garantindo a mesma disponibilidade do repositório da ECR-CV:

4.3.2.2. A cópia electrónica da DPC será publicada sempre que houver necessidade de se proceder a uma nova actualizaçao;

4.3.2.3. A LCR da ECR-CV, será publicada de acordo com o estabelecido no item 6.9.12;

4.3.2.4. Certificados da EC subordinada e certificados emitidos por esta, de acordo com a política definida na sua DPC.

4.3.3. CONTROLO DE ACESSO

4.3.3.1. A informação publicada pela ECR-CV estará disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso somente para leitura).

4.3.3.2. A ECR-CV implementou medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

4.4. AUDITORIA DE CONFORMIDADE

4.4.1. QUEM REALIZA AUDITORIA

4.4.1.1. Uma inspecção regular de conformidade a esta DPC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria de Sistemas da ECR-CV.

4.4.1.2. Para além das auditorias de conformidade, por determinação do CG da ICP-CV, serão efectuadas outras fiscalizações e investigações para assegurar a conformidade da ECR-CV com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria sem aviso prévio.

4.4.2. FREQUÊNCIA OU MOTIVO DA AUDITORIA

4.4.2.1. As auditorias de conformidade são realizadas anualmente de acordo com a legislação sendo que o Relatório de Auditoria de Segurança é entregue até 31 de Março[2].

[2] cf. Decreto Regulamentar n.º 18/2007, de 24 de Dezembro.

4.4.2.2. A ECR-CV deverá provar, com a auditoria e relatório de segurança anuais (produzidos pelo auditor de segurança acreditado), que a avaliação dos riscos foi assegurada, tendo sido identificadas e implementadas todas as medidas necessárias para a segurança de informação.

4.4.3. IDENTIDADE E QUALIFICAÇÕES DO AUDITOR

4.4.3.1. O auditor é uma pessoa ou organização, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infra-estruturas de chave pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança.

4.4.3.2. A Autoridade Credenciadora é responsável pela nomeação do pessoal que realiza a auditoria de conformidade e o CG da ICP-CV é responsável pela nomeação dos Auditores Externos.

4.4.3.3. O auditor externo deverá ser seleccionado no momento da realização de cada auditoria, devendo em termos gerais cumprir os seguintes requisitos:

a) Experiência em PKI, segurança e processos de auditoria em sistemas de informação;

b) Independência a nível orgânico da ECR-CV (para os casos de auditorias externas);

c) Credenciado pela Autoridade de Credenciação.

4.4.4. RELAÇÃO ENTRE A ECR-CV E O AUDITOR EXTERNO

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

4.4.4.2. O auditor de segurança deve garantir que nenhum membro da equipa executa funções parciais ou discriminatórias ligadas à ECR-CV nem que trabalhou para a mesma nos últimos três anos.

4.4.4.3. Na relação entre o auditor e a ECR-CV, deve estar garantida a inexistência de qualquer vínculo contratual.

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

4.4.4.5. O cumprimento do estabelecido na legislação em vigor sobre a protecção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais constantes dos ficheiros dos membros dos diversos grupos de trabalho afectos à ECR-CV assim como aos dados fornecidos no pedido de emissão de um certificado para Entidade Subordinada.

4.4.4.6. O auditor deve ser independente da ECR-CV e da ANAC, ter competência reconhecida, experiência e qualificações sólidas na área da segurança de informação no desempenho de auditorias de segurança e no uso do standard ISO/IEC 27002.

4.4.5. ÂMBITO DA AUDITORIA

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional, Políticas emitidas pela ICP-CV, com esta DPC e outras regras e normas, 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).

4.4.6. AUDITORIA COM RESULTADO DEFICIENTE

Se numa auditoria resultarem irregularidades devem ser adoptados os procedimentos seguintes :

a) Devem ser estipulados prazos para cumprir as irregularidades/não-conformidades detectadas;

b) Irregularidades e não-conformidades devem ser dadas a conhecer ao CG para servirem de referência a futuras fiscalizações.

4.5. SIGILO

4.5.1. CHAVES PRIVADAS

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

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

4.5.2. VERFICAÇÃO ESTADO DO CERTIFICADO

4.5.1.3. Antes de utilizarem um certificado, as partes confiantes têm, como responsabilidade verificar o estado de todo os certificados através das LCR.

4.5.1.4. As EC's subordinadas são sempre informadas sobre a alteração de estado dos seus certificados, e, em caso de suspensão ou revogação, qual o seu motivo.

4.5.3. QUEBRA DE SIGILO POR MOTIVOS LEGAIS

A ECR-CV deve disponibilizar, mediante ordem judicial ou por determinação legal, documentos, informações ou registos que estejam à sua guarda.

4.5.4. INFORMAÇÕES A TERCEIROS

Nenhum documento, informação ou registo que esteja sob a guarda da ECR-CV deve ser fornecido a terceiros excepto se estiverem devidamente identificados e autorizados a fazê-lo.

4.5.5. DIVULGAÇÃO POR SOLICITAÇÃO DO TITULAR

Não aplicável.

4.5.6. DIREITOS DE PROPRIEDADE INTELECTUAL

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID e DPC, bem como qualquer outro documento, são propriedade da ECR-CV e do Estado de Cabo Verde.

5. IDENTIFICAÇÃO E AUTENTICAÇÃO

5.1. REGISTO INICIAL

5.1.1. DISPOSIÇÕES LEGAIS

5.1.1.1. TIPOS DE NOMES

a) A atribuição de nomes segue a convenção determinada pela ICP-CV.
b) A operação dos certificados emitidos pela ECR-CV está sempre na dependência da ANAC.
c) O certificado da ECR-CV, é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

Tipo de Certificado	OID
DPC da ECR-CV	**2.16-.132.1.3.1.1**
Entidades de Certificação	**2.16.132.1.2.n**[3]

5.1.1.2. NECESSIDADE DE NOMES SIGNIFICATIVOS

A ECR-CV assegura que, na hierarquia de confiança da ICP-CV, não existem certificados que tendo o mesmo nome único identifiquem entidades (equipamento) distintas.

5.1.1.3. INTERPRETAÇÃO DE FORMATO DE NOMES

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

5.1.1.4. UNICIDADE DE NOMES

5.1.1.4.1. Os identificadores do tipo DN são únicos para cada uma das ECs subordinadas, não induzindo em ambiguidades.

5.1.1.4.2. De acordo com os seus processos de emissão, a ECR-CV e as suas ECs subordinadas rejeitam a emissão de certificados com o mesmo DN para titulares distintos.

5.1.1.5. PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

A ECR-CV reserva o direito de tomar todas as decisões no caso da existência de disputa de nomes resultante da igualdade de nomes entre diferentes pedidos de certificado.

[3] Em que n representa uma EC Subordinada

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

5.1.1.6. RECONHECIMENTO, AUTENTICAÇÃO DE MARCAS REGISTADAS

5.1.1.6.1. As entidades requisitantes de certificados, devem demonstrar que têm direito à utilização do nome requisitado, não podendo as designações usadas nos certificados emitidos pela ECR-CV e pelas Ecs infringir os direitos de propriedade intelectual de outros indivíduos ou entidades.

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

5.1.1.7. COMPROVAÇÃO DE POSSE DE CHAVE PRIVADA

5.1.1.7.1. Para as ECs, é considerado um mecanismo aceitável como método de comprovação da posse de chave privada a utilização do PKIX *Certificate Management Protocol* (CMP) definido no RFC 4210[5].

5.1.1.7.2. Na ECR-CV a comprovação da posse da chave privada será garantida através da presença física de um representante autorizado da entidade subordinada, na cerimónia de emissão desse tipo de certificados. Nessa cerimónia, o representante da entidade subordinada apresentará o pedido de certificado no formato PKCS#10[6].

5.1.1.8. AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO

Nada a assinalar.

5.1.1.9. AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO

5.1.1.9.1. O processo de autenticação da identidade de uma pessoa colectiva, deve obrigatoriamente garantir que a pessoa colectiva para quem vai ser emitido o certificado é quem na realidade diz ser e que a criação de assinatura, através de dispositivo de criação de assinatura, exige a intervenção de pessoas singulares que, estatutariamente, representam essa pessoa colectiva.

5.1.1.9.2. A ECR-CV responsabiliza-se pela guarda de toda a documentação utilizada para verificação da identidade da entidade que requisita um certificado, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, e garantindo, no caso dos seus representantes legais não se encontrarem na cerimónia de emissão de certificado, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

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

[6] cf. RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.

5.1.1.9.3. O documento[7] que serve de base ao registo da EC contém, entre outros, os seguintes elementos:

a) Documentos, para efeitos de identificação de EC e sua denominação legal;

b) Número de Identificação Fiscal, sede, objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem;

c) Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente, a representam;

d) Endereço e outras formas de contacto;

e) Indicação de que o certificado é emitido para a entidade, enquanto EC subordinada à ECR-CV, na hierarquia de confiança da ICP-CV, de acordo com a presente DPC;

f) Nome único (DN) a ser atribuído ao certificado de EC;

g) Informação, se necessário, relativa à identificação e aos poderes do(s) representante(s) nomeados pela entidade para estarem presentes na cerimónia de emissão do certificado de EC;

h) Outras informações relativas ao formato do pedido de certificado a serem apresentadas na cerimónia de emissão do certificado da EC.

5.1.1.10. VALIDAÇÃO DOS PODERES DE AUTORIDADE OU REPRESENTAÇÃO

Nada a assinalar.

5.2. CRITÉRIOS PARA INTEROPERABILIDADE

5.2.1. No caso de solicitação por parte de uma EC de acordos de interoperabilidade, tendo como base a certificação cruzada com outras infra estruturas de chaves públicas, a ECR-CV deve exigir no mínimo a seguinte documentação:

a) A Política de Certificados;

b) O último relatório de auditoria, demonstrando a total conformidade com o estabelecido na PC e na DPC;

c) Os parâmetros respeitantes a validação técnica da certificação cruzada;

5.2.2. Todos os pedidos de acordos de interoperabilidade devem ser devidamente aprovados pelo CG.

5.3. IDENTIFICAÇÃO E AUTENTICAÇÃO

5.3.1. RENOVAÇÃO DE CERTIFICADOS

[7] cf. PJ.ECRCV_53.2.1_0001_pt.doc. 2010, Formulário de emissão de certificado de EC subordinada da ECR-CV

A identificação e autenticação para a renovação de certificados são realizadas utilizando os procedimentos para a autenticação e identificação inicial.

5.3.2. RENOVAÇÃO DE CHAVES DE ROTINA

5.3.1.1. Não existe renovação de chaves, de rotina.

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

5.3.3. RENOVAÇÃO DE CHAVES, APÓS REVOGAÇÃO

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

5.4. PEDIDOS DE REVOGAÇÃO DE CHAVES

5.4.1. Qualquer entidade que integra a ICP-CV, pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro acto que recomende esta acção.

5.4.2. A ECR-CV guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efectua o pedido de revogação, que podem ser, entre outros:

a) Representante legal da Autoridade Credenciadora, com poderes de representação para o pedido de revogação de certificados;

b) Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos;

5.4.3. È utilizado formulário próprio[8] para solicitação de revogação de certificado, que contém, entre outras informações, os seguintes elementos de identificação da entidade que inicia o pedido de revogação:

a) Denominação legal;

b) Número de pessoa colectiva, sede, objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;

c) Nome completo, número de um documento de identificação que permita a identificação inequívoca da entidade (ou seu representante) que inicia o pedido de revogação;

d) Endereço e outras formas de contacto;

e) Indicação de pedido de revogação, indicando o nome único (DN) atribuído ao certificado, assim como a sua validade;

[8] cf. PJ.ECRCV_53.2.2_0001_pt.doc. 2010, Formulário de revogação de certificado emitido pela ECR-CV.

f) Indicação do motivo para revogação do certificado;

g) Informação das medidas que deverão ser adoptadas pela ECR-CV para revogar todos os certificados que emitiu, nos casos de revogação de certificado de uma EC subordinada.

6. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

6.1. PEDIDO DE CERTIFICADO

6.1.1. REQUISITOS

Devem ser cumpridos os seguintes requisitos quando é feito um pedido de certificado:

a) Conformidade com as políticas definidas pela ECR-CV;

b) Pedido de certificado mediante apresentação de um pedido de certificado PKCS#10 válido;

c) Nos casos das ECs, o processo de credenciação das mesmas já devem ter ocorrido e as mesmas já devem ter autorização para início de actividade.

6.1.2. QUEM PODE SUBSCREVER UM PEDIDO DE CERTIFICADO?

6.1.2.1. O certificado auto-assinado da ECR-CV apenas pode ser solicitado pela ANAC.

6.1.2.2. A entidade ou pessoa colectiva com poderes para representar a EC integrante ou candidata a integrar a ICP-CV.

6.1.3. PROCESSO DE REGISTO E RESPONSABILIDADES

O processo de registo de EC é constituído pelos seguintes passos, a serem efectuados pela EC requerente:

a) Geração do par de chaves (chave pública e privada) pela EC;

b) Geração do PKCS#10 correspondente pela EC;

c) Geração do hash (SHA-256[9]) do PKCS#10, em formato PEM, pela EC;

d) Arquivo do PKCS#10 e hash em suporte tecnológico não regravável (CD/DVD), pela EC;

e) Preenchimento pela EC de documento de validação da identidade da entidade, de acordo com alínea a) do número 5.1.9;

f) Envio do CD/DVD e do documento correctamente preenchido ao contacto da ECR-CV.

6.2. PROCESSAMENTO DO PEDIDO DE CERTIFICADO

6.2.1. REQUISITOS

6.2.1.1. Os pedidos de certificado, depois de recebidos pela ECR-CV, são considerados válidos se os seguintes requisitos forem cumpridos:

a) Recepção e verificação de toda a documentação e autorizações exigidas;

[9] cf. NIST FIPS PUB 180-1. 1995, *The Secure Hash Algorithm (SHA-256). National Institute of Standards and Technology, "Secure Hash Standard,", U.S. Department of Commerce.*

b) Verificação da identidade do requisitante;

c) Verificação da exactidão e integridade do pedido de certificado;

d) Criação e assinatura do certificado;

e) Disponibilização do certificado ao titular;

6.2.1.2. A secção 6.3 descreve detalhadamente todo o processo.

6.2.2. PROCESSO PARA A IDENTIFICAÇÃO E FUNÇÕES DE AUTENTICAÇÃO

6.2.2.1. A Administração de Segurança da ECR-CV executa a identificação e a autenticação de toda a informação necessária nos termos da secção 5.1.1.9.

6.2.2.2. A Administração de Segurança da ECR-CV aprova a candidatura para um certificado de Entidade de Certificação quando os seguintes critérios são preenchidos:

a) Identificação e autenticação bem sucedida, de toda a informação necessária nos termos da secção 5.1.1.9 (toda a documentação utilizada para verificação da identidade e de poderes de representação é guardada);

b) Formulário de pedido de emissão correctamente preenchido;

c) PKCS#10 válido.

6.2.2.3. Em qualquer outra situação, será rejeitada a candidatura para emissão de certificado.

6.2.2.4. Após a emissão do certificado, a Administração de Segurança da ECR-CV é responsável por entregar o certificado e restantes dados necessários pelo método "cara-a-cara" – tal acto é registado através do preenchimento e assinatura de formulário[10].

6.2.3. APROVAÇÃO OU RECUSA DE PEDIDOS DE CERTIFICADO

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos no ponto 6.2 quando tal não se verifique, é recusada a emissão do certificado.

6.2.4. PRAZO PARA PROCESSAR O PEDIDO DE CERTIFICADO

Após a aprovação do pedido de certificado, o certificado deverá ser emitido em não mais do que cinco (5) dias úteis.

6.3. EMISSÃO DE CERTIFICADO

[10] PJ.ECRCV_53.2.4_0001_pt.doc 2010, Formulário de recepção de certificado de EC subordinada da ECR-CV.

6.3.1. PROCEDIMENTO PARA A EMISSÃO DE CERTIFICADO DA ECR-CV

6.3.1.1. A emissão do certificado é efectuada por meio de uma cerimónia que decorre na zona de alta segurança da ECR-CV e, em que se encontram presentes:

a) Três (3) membros do Grupo de Trabalho – a segregação de funções não possibilita a presença de um número inferior de elementos;

b) Quaisquer observadores, aceites simultaneamente pelos membros do Grupo de Trabalho;

c) Dois (2) membros da Autoridade Credenciadora.

6.3.1.2. A cerimónia de emissão de certificado da ECR-CV é constituída pelos seguintes passos:

a) Identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que os membros do Grupo de Trabalho têm os poderes necessários para os actos a praticar;

b) Os membros do Grupo de Trabalho da ECR-CV efectuam o procedimento de arranque de processamento da ECR-CV e emitem o certificado;

c) Os membros do Grupo de Trabalho da ECR-CV arquivam o certificado num suporte tecnológico (não regravável);

d) A cerimónia de emissão fica terminada com a execução do procedimento de finalização de processamento da ECR-CV, pelos membros do Grupo de Trabalho da ECR-CV;

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

6.3.2. PROCEDIMENTOS PARA A EMISSÃO DE CERTIFICADO DE EC

6.3.2.1. A emissão do certificado é efectuada por meio de uma cerimónia que decorre na zona de alta segurança da ECR-CV e, em que se encontram presentes:

a) Os representantes legais da entidade subordinada requerente ou o(s) representante(s) nomeado(s) para esta cerimónia;

b) Três (3) membros dos Grupo de Trabalho – a segregação de funções não possibilita a presença de um número inferior de elementos;

c) Quaisquer observadores, aceites simultaneamente pelos membros dos Grupos de Trabalho e pelos representantes da entidade subordinada requerente.

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

a) Identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que o(s) representante(s) da entidade subordinada requerente e os membros dos Grupo de Trabalho têm os poderes necessários para os actos a praticar;

b) Representante(s) da entidade subordinada requerente entregam, em mão, o CD/DVD e o formulário de emissão do certificado aos membros do Grupo de Trabalho da ECR-CV. O formulário é datado e assinado pelos membros do Grupo de Trabalho que o devolvem ao(s) representantes da entidade subordinada requerente;

c) Os membros do Grupo de Trabalho da ECR-CV efectuam o procedimento de arranque de processamento da ECR-CV e emitem o certificado (correspondente ao PKCS#10 fornecido no CD/DVD) em formato PEM;

d) Os membros do Grupo de Trabalho da ECR-CV arquivam o certificado em formato PEM num CD/DVD e preenchem o formulário de recepção e aceitação de certificado[11], em duplicado;

6.3.2.3. Após a assinatura de ambas as cópias do formulário de recepção e aceitação de certificado pelo(s) representante(s) da entidade e pelos membros do Grupo de Trabalho, os membros do Grupo de Trabalho entregam o CD/DVD com o certificado em formato PEM ao(s) representante(s) da entidade subordinada;

6.3.2.4. A cerimónia de emissão fica terminada com a execução do procedimento de finalização de O representante toma conhecimento dos seus direitos e responsabilidades;

6.3.2.5. O representante toma conhecimento das funcionalidades e conteúdo do certificado;

6.3.2.6. O representante aceita formalmente o certificado e as suas condições de utilização assinando para o efeito o formulário de recepção de certificado de EC [12].

6.3.2.7. processamento da ECR-CV, pelos membros do Grupo de Trabalho da ECR-CV;

6.3.2.8. A emissão do certificado é efectuada na presença do responsável pela entidade titular do mesmo.

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

6.4. ACEITAÇÃO DO CERTIFICADO

6.4.1. PROCEDIMENTOS PARA A ACEITAÇÃO DE CERTIFICADO

6.4.1.1. O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) da EC, de acordo com cerimónia de emissão.

6.4.1.2. Note-se que antes de ser disponibilizado o certificado aos representantes, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e do certificado, é garantido que No termo de responsabilidade do titular constam os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo.

6.4.2. PUBLICAÇÃO DO CERTIFICADO

[11] cf. PJ.ECRCV_53.2.4_0001_pt.doc., Formulário de recepção de certificado de EC subordinada da ECR-CV.

[12] PJ.ECRCV_53.2.4_0001_pt.doc, Formulário de recepção de certificado de EC subordinada da ECR-CV

6.4.2.1. A ECR-CV disponibiliza o seu certificado no endereço electrónico identificado na secção 4.3.

6.4.2.2. Cada EC é responsável pela publicação do seu certificado no seu respectivo endereço electrónico (chave pública).

6.4.3. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO A OUTRAS ENTIDADES

Nada a assinalar.

6.5. USO DO CERTIFICADO E PAR DE CHAVES

6.5.1. USO DO CERTIFICADO E DA CHAVE PRIVADA PELO TITULAR

6.5.1.1. No âmbito da ICP-CV, o certificado da ECR-CV é utilizado apenas para:

a) A emissão de certificados para EC de primeiro nível; e

b) A assinatura da sua LCR.

6.5.2. USO DO CERTIFICADO E DA CHAVE PÚBLICA PELAS PARTES CONFIANTES

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

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

b) Ser responsável pela sua correcta utilização;

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

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

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

6.6. RENOVAÇÃO DE CERTIFICADOS SEM GERAÇÃO DE NOVO PAR DE CHAVES

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

6.6.2. Esta prática não é suportada na ICP-CV.

6.7. RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

6.7.1. DEFINIÇÃO

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

6.7.2. MOTIVO PARA A RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

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

a) O certificado está perto de expirar;

b) O suporte do certificado está danificado ou indicia deterioração que poderá comprometer a sua utilização a curto prazo.

6.7.3. QUEM PODE SOLICITAR UMA NOVA CHAVE PÚBLICA

Tal como na secção 6.1.2.

6.7.4. PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DE CERTIFICADO

Tal como na secção 6.2.

6.7.5. NOTIFICAÇÃO DA EMISSÃO DE NOVO CERTIFICADO AO TITULAR

Tal como na secção 6.3.2.

6.7.6. PROCEDIMENTOS PARA ACEITAÇÃO DE UM NOVO CERTIFICADO

Tal como na secção 6.4

6.7.7. PUBLICAÇÃO DE CERTIFICADO APÓS GERAÇÃO DE NOVO PAR DE CHAVES

Tal como na secção 6.4.2.

6.7.8. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO RENOVADO A OUTRAS ENTIDADES

Tal como na secção 6.4.3.

6.8. MODIFICAÇÃO DE CERTIFICADOS

Esta prática não é suportada no âmbito da ICP-CV.

6.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

6.9.1. ÂMBITO

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

6.9.1.2. Os certificados depois de revogados não podem voltar a ser válidos.

6.9.2. CIRCUNSTÂNCIAS PARA REVOGAÇÃO

Um certificado pode ser revogado por uma das seguintes razões:

a) Comprometimento ou suspeita de comprometimento da chave privada;

b) Perda da chave privada;

c) Incorrecções graves nos dados fornecidos;

d) Equipamento tecnológico deixa de ser utilizado no âmbito da ECR-CV;

e) Comprometimento ou suspeita de comprometimento da senha de acesso à chave privada (exemplo: PIN);

f) Comprometimento ou suspeita de comprometimento da chave privada da ECR-CV;

g) Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);

h) Revogação do certificado da ECR-CV;

i) Incumprimento por parte da ECR-CV ou titular das responsabilidades previstas na presente DPC;

j) 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;

k) Por resolução judicial ou administrativa.

6.9.3. QUEM PODE SUBMETER O PEDIDO DE REVOGAÇÃO

6.9.3.1. Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 6.9.2., as seguintes entidades:

a) O CG da ICP-CV;

b) A ECR-CV;

c) A Autoridade Credenciadora - ANAC;

d) As ECs integrantes da ICP-CV;

e) Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos previstos.

6.9.3.2. A ECR-CV guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efectua o pedido de revogação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado de EC.

6.9.4. PROCEDIMENTO PARA O PEDIDO DE REVOGAÇÃO

6.9.4.1. Todos os pedidos de revogação devem ser endereçados para a ECR-CV por escrito ou por mensagem electrónica assinada digitalmente, em formulário de pedido de revogação[13], observando o seguinte:

a) Identificação e autenticação da entidade que efectua o pedido de revogação, conforme secção 6.9.33;

b) Registo e arquivo do formulário de pedido de revogação;

c) Mediante o parecer do Conselho Executivo da ECR-CV, o responsável do organismo que tutela a ECR-CV, decide a aprovação ou recusa do pedido de revogação do certificado;

6.9.4.2. Sempre que se decidir revogar um certificado, a revogação é publicada na respectiva LCR.

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

a) Data do pedido de revogação;

b) Nome do titular do certificado (assinante);

c) Exposição pormenorizada dos motivos para o pedido de revogação;

d) Nome e funções da pessoa que solicita a revogação;

e) Informação de contacto da pessoa que solicita a revogação;

f) Assinatura da pessoa que solicita a revogação.

[13] PJ.ECRCV_53.2.2_0001_pt.doc, Formulário para pedido de revogação de certificado de EC do Estado

6.9.5. PRODUÇÃO DE EFEITOS DA REVOGAÇÃO

A revogação será feita de forma imediata. Após terem sido efectuados todos os procedimentos e seja verificado que o pedido é válido, o pedido não pode ser anulado.

6.9.6. PRAZO PARA PROCESSAR O PEDIDO DE REVOGAÇÃO

O pedido de revogação deve ser tratado de forma imediata, pelo que em caso algum poderá ser superior a 24 horas.

6.9.7. REQUISITOS DE VERIFICAÇÃO DA REVOGAÇÃO PELAS PARTES CONFIANTES

Antes de se utilizar um certificado, as partes confiantes têm como responsabilidade verificar o seu estado, através das LCR.

6.9.8. CIRCUNSTÂNCIAS PARA A SUSPENSÃO

Não é permitido a suspensão de certificados auto-assinados da ECR-CV nem dos certificados das EC's.

6.9.9. QUEM PODE SOLICITAR SUSPENSÃO

Nada a assinalar

6.9.10. PROCEDIMENTO PARA PEDIDO DE SUSPENSÃO

Nada a assinalar.

6.9.11. LIMITE DO PERÍODO DE SUSPENSÃO

Nada a assinalar.

6.9.12. FREQUÊNCIA DE EMISSÃO LCR

A ECR-CV publica uma nova LCR no repositório, sempre que haja uma revogação. Quando não haja alterações ao estado de validade dos certificados, ou seja, se nenhuma revogação tiver sido produzido, a ECR-CV disponibiliza uma nova LCR a cada 90 (noventa) dias.

6.9.13. PERÍODO MÁXIMO ENTRE A EMISSÃO E A PUBLICAÇÃO DA LCR

O período máximo entre a emissão e publicação da LCR não deverá ultrapassar as 3 horas.

6.9.14. DISPONIBILIDADE DE VERIFICAÇÃO ON-LINE DO ESTADO / REVOGAÇÃO DE CERTIFICADO

Não aplicável.

6.9.15. REQUISITOS DE VERIFICAÇÃO ON-LINE DE REVOGAÇÃO

Não aplicável.

6.9.16. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

Nada a assinalar.

6.9.17. REQUISITOS EM CASO DE COMPROMETIMENTO DE CHAVE PRIVADA

Quando se trata do comprometimento da chave privada de uma EC, o deverão ser adoptados os procedimentos descritos na secção 6.15.4.

6.10. SERVIÇOS SOBRE O ESTADO DO CERTIFICADO

6.10.1. CARACTERÍSTICAS OPERACIONAIS

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

6.10.2. DISPONIBILIDADE DO SERVIÇO

O serviço sobre o estado do certificado está disponível 24 horas por dia, 7 dias por semana.

6.11. 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.

6.12. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

6.12.1. TIPO DE EVENTOS REGISTADOS

6.12.1.1. Pedido, emissão, renovação, re-emissão e revogação de certificados;

6.12.1.2. Publicação de LCR;

6.12.1.3. Eventos relacionados com segurança, incluindo:

a) Tentativas de acesso (com e sem sucesso) a recursos sensíveis da Entidade de Certificação;

b) Operações realizadas por membros dos Grupos de Trabalho;

c) Dispositivos físicos de segurança de entrada / saída dos vários níveis de segurança;

6.12.1.4. As entradas nos registos incluem a informação seguinte:

a) Data e hora do evento;

b) Identidade do sujeito que causou o evento;

c) Categoria do evento;

d) Descrição do evento.

6.12.2. FREQUÊNCIA DA AUDITORIA DE REGISTOS

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

6.12.3. PERÍODO DE RETENÇÃO DOS REGISTOS DE AUDITORIA

Os registos são mantidos por um mínimo de 2 (dois) meses e posteriormente arquivados por 20 (vinte) anos.

6.12.4. PROTECÇÃO DOS REGISTOS DE AUDITORIA

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

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

6.12.5. PROCEDIMENTOS, PARA A CÓPIA DE SEGURANÇA DOS REGISTOS

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade, e a intervalos de tempo não superiores a uma semana.

6.12.6. SISTEMA DE RECOLHA DE REGISTOS (INTERNO / EXTERNO)

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

6.12.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

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

6.12.8. AVALIAÇÃO DE VULNERABILIDADES

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

6.13. ARQUIVO DE REGISTOS

6.13.1. TIPO DE DADOS ARQUIVADOS

6.13.1.1. Todos os dados auditáveis são arquivados, assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

6.13.1.2. Os dados auditáveis serão entre outros:

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR.

6.13.2. PERÍODO DE RETENÇÃO EM ARQUIVO

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

6.13.3. PROTECÇÃO DOS ARQUIVOS

Os arquivos são protegidos de modo a que:

a) Apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo;

b) O arquivo é protegido contra qualquer modificação ou tentativa de o remover;

c) O arquivo é protegido contra a deterioração do media onde é guardado, através de migração periódica para media novo;

d) O arquivo é protegido contra a obsolescência do hardware, sistemas operativos e outro software, pela conservação do hardware, sistemas operativos e outro software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal; e

e) Os arquivos são guardados em ambientes seguros.

6.13.4. PROCEDIMENTOS PARA AS CÓPIAS DE SEGURANÇA DO ARQUIVO

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

6.13.5. REQUISITOS, PARA VALIDAÇÃO CRONOLÓGICA DOS REGISTOS

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

6.13.6. SISTEMA DE RECOLHA DE DADOS DE ARQUIVO (INTERNO / EXTERNO)

Os sistemas de recolha de dados de arquivo são internos.

6.13.7. PROCEDIMENTOS DE RECUPERAÇÃO E VERIFICAÇÃO DE INFORMAÇÃO ARQUIVADA

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

6.14. RENOVAÇÃO DE CHAVES

As ECs com certificados válidos podem requerer a renovação do respectivo par de chaves, desde que com a geração de novo par de chaves.

6.15. RECUPERAÇÃO EM CASO DE DESASTRE OU COMPROMETIMENTO

6.15.1. ÂMBITO

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

6.15.2. PROCEDIMENTOS EM CASO DE INCIDENTE OU COMPROMETIMENTO

Cópias de segurança das chaves privadas da EC (geradas e mantidas de acordo com a secção 8.16) e dos registos arquivados (secção 6.12 são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento).

6.15.3. CORRUPÇÃO DOS RECURSOS INFORMÁTICOS, DO SOFTWARE E/OU DOS DADOS

6.15.3.1. 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.

6.15.3.2. 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 ECR-CV suspenderá os seus serviços e notificará ao CG da ICP-CV.

6.15.4. COMPROMETIMENTO DA CHAVE PRIVADA DA ENTIDADE

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

a) Revogação do certificado da ECR-CV e de todos os certificados emitidos no "ramo" da hierarquia de confiança da ECR-CV;

b) Notificação às Entidades de Certificação, CG da ICP-CV, Autoridade Credenciadora e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da ECR-CV;

c) Geração de novo par de chaves para a ECR-CV e emissão de novo certificado;

d) Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da ECR-CV.

6.15.5. CAPACIDADE DE CONTINUIDADE DA ACTIVIDADE EM CASO DE DESASTRE

A ECR-CV dispõe dos recursos de computação, *software*, cópias de segurança e registos, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) após desastres de causa natural ou de natureza diversa . Estes recursos estão arquivados nas suas instalações de segurança secundárias.

6.16. PROCEDIMENTOS EM CASO DE EXTINÇÃO DA ECR-CV

6.16.1. Em caso de cessação de actividade como prestador de serviços de Certificação, a ECR-CV deve, com uma antecedência mínima de 3 (três) meses, proceder às seguintes acções:

a) Informar às EC, titulares de certificados em vigor;

b) Informar às EC, titulares qual a entidade para a qual é transmitida a sua documentação;

c) Revogar todos os certificados emitidos, colocando a sua documentação à guarda da ANAC;

d) Efectuar uma notificação final à sociedade cívil2 (dois) dias antes da cessação formal da actividade;

e) Garantir a transferência (para retenção por outra organização) de toda a informação relativa à actividade de certificação eletrónica, nomeadamente, chave da ECR-CV, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

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

6.17. RETENÇÃO E RECUPERAÇÃO DE CHAVES (KEY ESCROW)

6.17.1. CHAVE DA ECR-CV

A ECR-CV só efectua a retenção da sua chave privada.

6.17.2. POLÍTICAS E PRÁTICAS DE RECUPERAÇÃO DE CHAVES

6.17.2.1. A chave privada da ECR-CV é armazenada num token hardware de segurança, sendo efectuada uma cópia de segurança utilizando uma ligação directa hardware a hardware

entre os dois tokens de segurança. A geração da cópia de segurança é o último passo da emissão de um novo par de chaves da ECR-CV.

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

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

6.17.2.4. A cópia de segurança da chave privada da ECR-CV pode ser recuperada no caso de mau funcionamento da chave original. A cerimónia de recuperação da chave utiliza os mesmos mecanismos de autenticação de dois factores e com múltiplas pessoas, que foram utilizados na cerimónia de cópia de segurança.

6.17.3. ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVES DE SESSÃO

Nada a assinalar.

7. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

7.1. RESUMO

7.1.1. A ECR-CV implementou várias regras e políticas incidindo sobre controlos físicos, de procedimentos e humanos, que suportam os requisitos de segurança constantes desta DPC.

7.1.2. Esta secção descreve sucintamente os aspectos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos titulares, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança nos certificados, pois qualquer falta de segurança pode comprometer as operações da ECR-CV.

7.2. MEDIDAS DE SEGURANÇA FÍSICA

7.2.1. CONSTRUÇÃO E LOCALIZAÇÃO FÍSICA DAS INSTALAÇÕES DA EC

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

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

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

a) Paredes em alvenaria, betão ou tijolo;

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

c) Inexistência de janelas;

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

7.2.1.4. Adicionalmente, as seguintes condições de segurança são garantidas no ambiente da ECR-CV:

a) Perímetros de segurança claramente definidos;

b) Paredes, chão e tecto em alvenaria, sem janelas, que impedem acessos não autorizados;

c) Trancas e fechaduras anti-roubo de alta segurança nas portas de acesso ao ambiente de segurança;

d) O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;

e) 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.

7.2.2. ACESSO FÍSICO AO LOCAL

7.2.2.1. Os sistemas da ECR-CV estão protegidos por 6 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança),

garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

7.2.2.2. Actividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer actividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita de alta segurança. O acesso a cada nível de segurança requer o uso de um cartão magnético de autenticação (amarelo para o edifício, e vermelho para os outros níveis). Acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias. Os sistemas devem estar integrados, funcionamento de forma ininterrupta 24 horas, todos os dias do ano.

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

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

7.2.2.5. Deve existir um livro para registo manual dos acessos, de visitantes devidamente autorizados, e de todas as actividades e cerimónias que ocorram no seu interior.

7.2.3. ENERGIA E AR CONDICIONADO

O ambiente seguro da ECR-CV possui equipamento redundante, que garante condições de funcionamento 24 horas por dia, 7 dias por semana, o seguinte:

a) Alimentação de energia garantindo alimentação contínua ininterrupta com a potência suficiente para manter autonomamente a rede eléctrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações eléctricas que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia, e geradores de electricidade a diesel); e

b) Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correcto funcionamento de todos os equipamentos electrónicos e mecânicos presentes dentro do ambiente. Um sensor de temperatura activa um alerta GSM sempre que a temperatura atinge valores anormais. Este alerta GSM consiste em telefonemas com uma mensagem previamente gravada, para os elementos da equipa de manutenção.

7.2.4. EXPOSIÇÃO À ÁGUA

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

7.2.5. PREVENÇÃO E PROTECÇÃO CONTRA INCÊNDIO

O ambiente seguro da ECR-CV 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 seguintes requisitos:

a) Sistemas de detecção e alarme de incêndio estão instalados nos vários níveis físicos de segurança;

b) 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;

c) Procedimentos de emergência bem definidos, em caso de incêndio;

d) Os materiais da sala e portas utilizadas devem ser de material não combustível e resistentes ao fogo.

7.2.6. SALVAGUARDA DE SUPORTES DE ARMAZENAMENTO

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

7.2.6.2. 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.

7.2.6.3. Em situações que impliquem a deslocação física de hardware de armazenamento de dados (i.e., discos rígidos,...) para fora da zona de alta segurança, por motivos que não o arquivo de cópias de segurança, cada elemento 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).

7.2.7. ELIMINAÇÃO DE RESÍDUOS

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

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

7.3. INSTALAÇÕES EXTERNAS (ALTERNATIVA), PARA RECUPERAÇÃO DE SEGURANÇA

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

7.4. MEDIDA DE SEGURANÇA DOS PROCESSOS

7.4.1. A actividade da ECR_CVdepende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque:

a) 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;

b) 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;

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

7.4.2. 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.

7.5. FUNÇÕES DE CONFIANÇA

7.5.1. PESSOAS AUTENTICADAS

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

7.5.1.2. No âmbito da ECR-CV os papéis de confiança foram agrupados em sete categorias diferentes (que correspondem a sete Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efectuadas por diferentes pessoas devidamente autenticadas, pertencentes a diferentes Grupos de Trabalho.

7.5.2. GRUPO DE TRABALHO DE ADMINISTRAÇÃO DE SEGURANÇA

7.5.2.1. O Grupo de Trabalho de Administração de Segurança é responsável por propor, gerir e implementar todas as políticas da EC, assegurando que se encontram actualizadas, e garantir que toda a informação indispensável ao funcionamento e auditoria da EC se encontra disponível[14] ao longo do tempo. O Grupo de Trabalho de Administração de Segurança assume também a função de Operação de HSM.

7.5.2.2. As responsabilidades deste grupo incluem:

a) Gerir o Ambiente de Administração de Segurança.

b) Assumir o papel de Consultor de Sistemas conforme alínea a) do nº 1 do Artigo 6º do Decreto-Lei nº44/2009.

c) Definir e gerir todas as políticas da EC e garantir que se encontram actualizadas e adaptadas à sua realidade.

d) Garantir implementação das políticas definidas.

e) Assegurar que as PCs da EC são suportadas pela DPC da EC.

f) Assegurar que todos os documentos relevantes e relacionados, directa ou indirectamente, com o funcionamento da EC e existentes em formato papel[15] se encontram armazenados no Ambiente de Informação.

g) Gerir e controlar os sistemas de segurança física, incluindo acessos, do ambiente de produção.

h) Explicar todos os mecanismos de segurança aos funcionários que devam conhecê-los e de consciencializá-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de seguranças estabelecidas.

i) Calendarizar cerimónias para testes, formações e auditoria dos sistemas de informação;

j) Configurar os acessos à aplicação da EC (grupos, regras, logs);

[14] Para elementos devidamente autorizados

[15] Os procedimentos a adoptar em relação aos documentos em formato electrónico serão definidos após a concretização do *Business Continuity Plan*

k) Configurar perfis de certificados na aplicação da EC;

l) Activação da interface de operação da EC;

m) Activação de chaves para sua utilização. Isto significa que cada vez que se inicie a EC, é necessário a inserção dos cartões de operador, associados às chaves;

n) Autorização para a geração de chaves da aplicação. Esta operação é requerida durante a cerimónia de geração de chaves para a EC;

o) Arranque do interface de configuração da ECR-CV.

7.5.3. GRUPO DE TRABALHO DE ADMINISTRAÇÃO DE REGISTO

7.5.3.1. O Grupo de Trabalho de Administração de Registo é responsável por reportar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC assim como todos os incidentes sucedidos. Também é missão deste grupo operar a EC no que diz respeito à emissão, suspensão e revogação de certificados.

7.5.3.2. As responsabilidades deste grupo são emitir, suspender e revogar certificados.

7.5.4. GRUPO DE TRABALHO DE ADMINISTRAÇÃO DE SISTEMAS

7.5.4.1. O Grupo de Trabalho de Administração de Sistemas é responsável por instalar, configurar e fazer a manutenção (hardware e software) da EC, sem afectar a segurança da aplicação.

7.5.4.2. As responsabilidades deste grupo são:

a) Manter um inventário actualizado de todos os produtos relacionados com a EC;

b) Instalar, interligar e configurar o *hardware* da EC;

c) Instalar e configurar o *software* de base da EC;

d) Gerir e actualizar os produtos instalados;

e) Preparar comunicados sobre as palavras-chave iniciais;

f) Preparar comunicados sobre as Hash do(s) CD(s) de instalação utilizados.

7.5.5. GRUPO DE TRABALHO DE OPERAÇÃO DE SISTEMAS

7.5.5.1. O Grupo de Trabalho de Operação de Sistemas é responsável por operar diariamente os sistemas, realizando cópias de segurança e reposição de informação, caso necessário.

7.5.5.2. As responsabilidades deste grupo são:

a) Realizar as tarefas de rotina da EC, incluindo operações de cópias de segurança dos seus sistemas;

b) Gerir o Ambiente de Operação.

7.5.6. GRUPO DE TRABALHO DE AUDITORIA DE SISTEMAS

7.5.6.1. O Grupo de Trabalho de Auditoria de Sistemas é responsável por efectuar a auditoria interna a todas as acções relevantes e necessárias para assegurar a operacionalidade da EC.

7.5.6.2. As responsabilidades deste grupo são:

a) Auditar a execução e confirmar a exactidão dos processos e cerimónias da EC;

b) Registar todas as operações sensíveis;

c) Investigar suspeitas de fraudes procedimentais;

d) Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;

e) Registar todos os procedimentos passíveis de auditoria;

f) Registar os resultados de todas as acções por si realizadas;

g) Validar que todos os recursos usados são seguros;

h) Verificação periódica, da integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respectivos[16] e que estão devidamente identificados;

i) Inspeccionar a configuração estabelecida pelas tarefas de administração e os eventos registados;

j) Estar devidamente credenciados como Auditores Internos pela Autoridade Credenciadora.

7.5.7. CONSELHO EXECUTIVO (CONSULTOR DE SISTEMAS)

7.5.7.1. É responsável pela nomeação dos membros dos restantes grupos[17] e pela tomada de decisões de nível crítico para a EC. Este grupo deve ser constituído por um mínimo de 4 (quatro) membros.

7.5.7.2. As responsabilidades deste grupo são:

a) Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Administração de Segurança;

b) Pedir a aprovação de Políticas ao CG da ICP-CV;

c) Designar os membros dos restantes grupos de trabalho (à excepção do Grupo de Trabalho de Instalação, do Grupo de Trabalho de Auditoria e do Grupo de Trabalho de Custódia);

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

[17] À excepção do Grupo de Trabalho de Instalação, do Grupo de Trabalho de Auditoria de Sistemas e do Grupo de Trabalho de Custódia

d) Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados.

7.5.8. GRUPO DE TRABALHO DE CUSTÓDIA

7.5.8.1. 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[18]. 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.

7.5.8.2. As responsabilidades deste grupo são:

a) Gestão do "Ambiente de Custódia" respectivo;

b) Custódia de artefactos sensíveis (tokens de autenticação, etc.) usando os meios adequados que respondam às necessidades de segurança respectivas;

c) Disponibilização segura destes itens a membros de grupos autorizados e explicitamente indicados com permissões de acesso a esses itens, após o cumprimento dos procedimentos apropriados de segurança.

7.6. NÚMERO DE PESSOAS EXIGIDAS POR TAREFA

7.6.1. 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.

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

7.7. IDENTIFICAÇÃO E AUTENTICAÇÃO, PARA CADA FUNÇÃO

Cada membro de cada grupo autentica-se em conta própria para acesso à máquina sendo que o acesso a aplicação da ECR-CV é feito com recurso à utilização de um certificado digital próprio emitido para o efeito.

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

7.8. FUNÇÕES QUE REQUEREM SEPARAÇÃO DE RESPONSABILIDADES

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

Incompatibilidade de Funções						
Grupo/Subgrupo	**Administração de Segurança**	**Administração de Registo**	**Administração de Sistemas**	**Operação de Sistemas**	**Auditoria de Sistemas**	**Conselho Executivo**
Administração de Segurança						
Administração de Registo						
Administração de Sistemas						
Operação de Sistemas						
Auditoria de Sistemas						
Conselho Executivo						

7.9. MEDIDAS DE SEGURANÇA DE PESSOAL

7.9.1. A admissão de pessoal com funções de confiança nos Grupos de Trabalho é apenas possível se:

a) Forem nomeados formalmente para a função;

b) São pessoas idóneas;

c) Apresentarem provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas dos Grupos de Trabalho;

d) Tiverem recebido formação e treino adequado para o desempenho da respectiva função;

e) Garantir que o funcionário não revela informação sensível sobre a EC ou dados de identificação dos titulares;

f) Garantir que o funcionário conhece os termos e condições para o desempenho da respectiva função;

g) Garantir que o funcionário não desempenha funções que possam causar conflito com as suas responsabilidades nas actividades da EC.

7.9.2. Adicionalmente, o Grupo de Trabalho de Auditoria de Sistemas deve ser constituído por elementos devidamente credenciados pela Autoridade Credenciadora como Auditores Internos.

7.10. REQUISITOS DE ADMISSÃO

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.

7.11. 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 inclui:

a) Confirmação de identificação, usando documentação emitida por fontes fiáveis;

b) Investigação de registos criminais;

c) Verificação de situação de crédito;

d) Verificação de histórico de empregos anteriores;

e) Comprovativo de escolaridade e de residência.

7.12. REQUISITOS DE FORMAÇÃO E TREINO

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

7.12.2. 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 actividade;

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

7.13. FREQUÊNCIA E REQUISITOS PARA ACÇÕES DE RECICLAGEM

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

a) Sempre que existe qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afecto às EC;

b) Sempre que são introduzidas alterações no presente documento são realizadas sessões de reciclagem aos elementos da ECR-CV.

7.14. FREQUÊNCIA E SEQUÊNCIA DA ROTAÇÃO DE FUNÇÕES

Nada a assinalar.

7.15. SANÇÕES PARA ACÇÕES NÃO AUTORIZADAS

7.15.1. Consideram-se acções não autorizadas todas as acções que desrespeitem a Declaração de Práticas de Certificação, quer sejam realizadas de forma deliberada ou sejam ocasionadas por negligência, imperícia ou imprudência.

7.15.2. São aplicadas sanções de acordo com as regras da ICP-CP e a legislação nacional, a todos os indivíduos que realizem acções não autorizadas ou que façam uso não autorizado dos sistemas.

7.16. REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

7.16.1. Consultores ou prestadores de serviços independentes tem permissão de acesso à zona de alta segurança desde de que estejam sempre acompanhados e directamente supervisionados pelos membros do Grupo de Trabalho.

7.16.2. Os procedimentos de verificação de antecedentes a aplicar nestas situações são os mesmos que são indicados na secção 7.11.

7.17. 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.

8. MEDIDAS DE SEGURANÇA TÉCNICA

8.1. ÂMBITO

Esta secção define as medidas de segurança implementadas para a ECR-CV de forma a proteger chaves criptográficas geradas por esta, e respectivos dados de activação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras

assim como dados de activação estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

8.2. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

8.2.1. GERAÇÃO DO PAR DE CHAVES

8.2.1.1. A geração dos pares de chaves da ECR-CV é processada de acordo com os requisitos e algoritmos definidos nesta DPC.

8.2.1.2. A geração de chaves criptográficas da ECR-CV é feita 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

8.2.1.3. A ECR-CV funciona em modo off-line e o seu certificado é auto-assinado. O respectivo par de chaves é gerado em hardware criptográfico, cumprindo requisitos FIPS 140-2 nível 3 e/ou Common Criteria EAL 4+ e, efectua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o hardware.

8.2.1.4. 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 efectuadas apenas usando hardware, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perda de dados, possa haver uma recuperação total e segura das chaves.

8.2.2. ENTREGA DA CHAVE PRIVADA AO TITULAR

Não se aplica.

8.2.3. ENTREGA DA CHAVE PÚBLICA AO EMISSOR DO CERTIFICADO

8.2.1.5. No caso do certificado auto assinado da ECR-CV não se procede à entrega.

8.2.1.6. A chave pública das EC é disponibilizada à ECR-CV, de acordo com os procedimentos indicados na secção 6.3.

8.2.4. ENTREGA DA CHAVE PÚBLICA DA EC ÀS PARTES CONFIANTES

A chave pública da ECR-CV será disponibilizada através do seu certificado, conforme secção 6.4.2.

8.2.5. DIMENSÃO DAS CHAVES

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:

a) 4096 bits RSA para a chave da ECR-CV;

b) 4096 bits RSA para a chave das EC subordinadas.

8.2.6. PARÂMETROS DA CHAVE PÚBLICA E VERIFICAÇÃO DA QUALIDADE

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

8.2.1.8. As chaves da EC são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos nas normas ISO 9564-1 e 11568-5 respectivamente.

8.2.7. FINS A QUE SE DESTINAM AS CHAVES (CAMPO "KEY USAGE" X.509 V3)

A chave privada da ECR-CV é utilizada apenas para assinatura do seu próprio certificado, dos certificados das ECs subordinadas e da sua LCR.

8.3. PROTECÇÃO DA CHAVE PRIVADA E CARACTERÍSTICAS DO MÓDULO CRIPTOGRÁFICO

Nesta secção são considerados os requisitos para protecção da chave privada e para os módulos criptográficos da ECR-CV, implementados com a combinação de controlos físicos, lógicos e procedimentos, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas da ECR-CV.

8.4. NORMAS E MEDIDAS DE SEGURANÇA DO MÓDULO CRIPTOGRÁFICO

8.4.1. SEGURANÇA FÍSICA

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

a) Common Criteria EAL 4+; e/ou

b) FIPS 140-2, nível 3;

8.4.2. CERTIFICAÇÕES REGULAMENTARES

a) U/L 1950 & CSA C22.2 safety compliant;

b) FCC Part 15 – Class B;

c) Certificação ISO – 9002;

8.4.3. AUTENTICAÇÃO

Autenticação de dois factores.

8.5. CONTROLO MULTI-PESSOAL (M DE N) PARA A CHAVE PRIVADA

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

8.5.2. A ECR-CV implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efectuar operações criptográficas sensíveis na sua EC.

8.5.3. Os dados de activação necessários para a utilização da chave privada da ECR-CV são divididos em várias partes, acessíveis e à responsabilidade de diferentes membros do Grupo de Trabalho. Um determinado número destas partes (m=2) do número total de partes (n=6) é necessário para activar a chave privada da ECR-CV guardada no módulo criptográfico em hardware. São necessárias duas (m) partes para a activação da chave privada da ECR-CV.

8.6. RETENÇÃO DA CHAVE PRIVADA (KEY ESCROW)

8.6.1. Não é permitida, no âmbito da ICP-CV, a retenção da chave privada quando aplicado a individuos.

8.6.2. A retenção da chave privada da ECR-CV é explicada na secção 6.17.

8.7. CÓPIA DE SEGURANÇA DA CHAVE PRIVADA

A chave privada da ECR-CV tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original.

8.8. ARQUIVO DA CHAVE PRIVADA

As chaves privadas da ECR-CV, alvo de cópias de segurança, são arquivadas conforme identificado na secção 6.17.

8.9. TRANSFERÊNCIA DA CHAVE PRIVADA PARA/DO MÓDULO CRIPTOGRÁFICO

8.9.1. As chaves privadas da ECR-CV não são exportáveis a partir do *token* criptográfico *FIPS 140*-2 nível 3.

8.9.2. Mesmo se for feito uma cópia de segurança das chaves privadas da ECR-CV para um outro *token* criptográfico, essa cópia é feita directamente, *hardware* para *hardware*, de forma a garantir o transporte das chaves entre módulos numa transmissão cifrada.

8.10. ARMAZENAMENTO DA CHAVE PRIVADA NO MÓDULO CRIPTOGRÁFICO

As chaves privadas da ECR-CV são armazenadas de forma cifrada nos módulos do *hardware* criptográfico.

8.11. PROCESSO PARA ACTIVAÇÃO DA CHAVE PRIVADA

8.11.1. A ECR-CV é uma Entidade de Certificação que opera off-line, cuja chave privada é activada quando o seu sistema é ligado. Esta activação é efectivada através da autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação de dois factores (consola de autenticação portátil e chaves de activação com código PIN associado), em que várias pessoas (membros dos grupos de trabalho), cada uma delas possuindo uma chave de activação, são obrigadas a autenticar-se antes que seja possível efectuar a cópia de segurança.

8.11.2. Para a activação das chaves privadas da ECR-CV é necessária, no mínimo, a intervenção de 3 elementos do Grupo de Trabalho. Uma vez a chave activada, esta permanecerá assim até que o processo de desactivação seja executado.

8.12. PROCESSO PARA DESACTIVAÇÃO DA CHAVE PRIVADA

8.12.1. A chave privada da ECR-CV é desactivada quando o seu sistema é desligado.

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

8.13. PROCESSO PARA DESTRUIÇÃO DA CHAVE PRIVADA

8.13.1. As chaves privadas da ECR-CV (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).

8.13.2. A ECR-CV, garante que do processo de destruição das chaves privadas 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 sua EC.

8.14. AVALIAÇÃO/NÍVEL DO MÓDULO CRIPTOGRÁFICO

Descrito na secção 8.4.

8.15. OUTROS ASPECTOS DA GESTÃO DO PAR DE CHAVES

8.15.1. ARQUIVO DA CHAVE PÚBLICA

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

8.15.2. PERÍODOS DE VALIDADE DO CERTIFICADO E DAS CHAVES

8.15.2.1. 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.

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

a) O certificado da ECR-CV tem uma validade de 24 anos, com renovação a cada 12 anos;

b) Os certificados das EC tem uma validade de 12 anos, com renovação a cada 6 anos (tempo máximo permitido).

8.16. DADOS DE ACTIVAÇÃO

8.16.1. GERAÇÃO E INSTALAÇÃO DOS DADOS DE ACTIVAÇÃO

Os dados de activação necessários para a utilização da chave privada da ECR-CV são divididos em várias partes (guardadas em chaves de activação), ficando à responsabilidade de diferentes membros do Grupo de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves e obedecem aos requisitos definidos pela norma FIPS 140-2 nível 3.

8.16.2. PROTECÇÃO DOS DADOS DE ACTIVAÇÃO

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

8.16.1.2. As chaves privadas da ECR-CV são guardadas, de forma cifrada, em token criptográfico.

8.16.3. OUTROS ASPECTOS DOS DADOS DE ACTIVAÇÃO

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

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

8.17. MEDIDAS DE SEGURANÇA INFORMÁTICA

8.17.1. REQUISITOS TÉCNICOS ESPECÍFICOS

8.17.1.1. O acesso aos servidores da ECR-CV é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso.

8.17.1.2. A ECR-CV tem um funcionamento *off-line*, sendo desligada no fim de cada emissão de certificado ou de qualquer outra intervenção técnica necessária e que cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

8.17.2. AVALIAÇÃO/NÍVEL DE SEGURANÇA

8.17.2.1. Os vários sistemas e produtos empregues pela ECR-CV são fiáveis e protegidos contra modificações.

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

8.18. CICLO DE VIDA DAS MEDIDAS TÉCNICAS DE SEGURANÇA

8.18.1. MEDIDAS DE DESENVOLVIMENTO DO SISTEMA

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

8.18.1.2. É fornecida metodologia auditável que permite verificar que o software da ECR-CV 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.

8.18.2. MEDIDAS PARA A GESTÃO DA SEGURANÇA

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

8.18.3. CICLO DE VIDA DAS MEDIDAS DE SEGURANÇA

As operações de actualização e manutenção dos produtos e sistemas da ECR-CV, seguem o mesmo controlo que o equipamento original e são instalados pelos membros do Grupo de Trabalho com adequada formação para o efeito, seguindo os procedimentos definidos para o efeito.

8.19. MEDIDAS DE SEGURANÇA DA REDE

A rede da ECR-CV não se encontra ligada a outra rede, fora da sede da ANAC.

8.20. VALIDAÇÃO CRONOLÓGICA (TIME-STAMPING)

Certificados, LCRs e outras entradas na base de dados contêm sempre informação sobre a data e hora dessas entradas, determinadas através de fonte de tempo segura. Tal informação não é baseada em mecanismos criptográficos.

9. PERFIS DE CERTIFICADO, CRL E OCSP

9.1. PERFIS DE CERTIFICADO DA ECR-CV

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

9.1.2. 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.

9.1.3. 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.

9.1.4. O formato de todos os certificados emitidos pela ECR-CV está em conformidade com:

a) Recomendação ITU.T X.509[19], versão 3;

b) RFC 5280[20];

c) Política de Certificados da ICP-CV.

9.1.5. O certificado da ECR-CV é o único certificado auto-assinado da ICP-CV, e possui validade de 24 (vinte e quatro) anos, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-CV.

9.2. NÚMERO DE VERSÃO

O certificado da ECR-CV implementa a versão 3 de certificado do padrão ITU X.509.

9.3. RESTRIÇÕES DE NOME

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

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

Não são admitidos caracteres especiais ou de acentuação nos campos do DN.

9.4. OID DA DPC

O OID desta DPC é 2.16.132.1.3.1.1

9.5. USO DA EXTENSÃO "POLICY CONSTRAINTS"

Nada a assinalar.

9.6. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Nada a assinalar.

9.7. SEMÂNTICA DE PROCESSAMENTO PARA AS EXTENSÕES CRÍTICAS DE PC

Nada a assinalar.

9.8. EXTENSÕES DE CERTIFICADO DA ECR-CV

9.8.1. As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

Componente do Certificado		Secção no RFC 3280	Valor	Tipo[21]	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização de certificados ITU-T X.509 versão 3.
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"ANAC-Agencia Nacional das Comunicacoes"		
	Common Name (CN)		" Entidade de Certificacao Raiz de Cabo Verde 001"		
	Validity	4.1.2.5		m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralisedTime*
	Not Before		<data de emissão>		
	Not After		<data de emissão + 24 anos>		Validade de 24 anos com renovação a cada 12 anos.
	Subject	4.1.2.6	<mesmo que *Issuer*>	m	Quando o *subject* é uma EC auto-assinada, tem que conter um DN igual ao *Issuer*.
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).

[21] O perfil utilize a terminologia seguinte para cada um dos tipos de campo no certificado X.509:
m – mandatório (o campo TEM que estar presente)
o – opcional (o campo PODE estar presente)
c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

Componente do Certificado		Secção no RFC 3280	Valor	Tipo	Comentários
	Algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.[22]
	subjectPublicKey		<Chave Pública com modulus n de 4096 bits>		
	Unique Identifiers	4.1.2.8			O "*unique identifiers*" está presente para permitir a possibilidade de reutilizar os nomes do *subject* e/ou *issuer* 20
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA.
	Digital Signature		"0" seleccionado		
	Non Repudiation		"0" seleccionado		
	Key Encipherment		"0" seleccionado		
	Data Encipherment		"0" seleccionado		

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

Componente do Certificado		Secção no RFC 3280	Valor	Tipo	Comentários
	Key Agreement		"0" seleccionado		
	Key Certificate Signature		"1" seleccionado		
	CRL Signature		"1" seleccionado		
	Encipher Only		"0" seleccionado		
	Decipher Only		"0" seleccionado		
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		2.16.132.1.3.1.1	m	Identificador da Declaração de Práticas de Certificação da ECR-CV
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.ecrcv.cv/pub/pol/ec_raiz_dpc_001_pt.html	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Declaração de Práticas de Certificação publicada pela ECR-CV. O apontador está na forma de um URI."
	Basic Constraints	4.2.1.10		mc	Esta extensão é marcada CRÍTICA.
	CA		TRUE		Indica o tipo de Entidade a quem se destina o certificado; restrição básica, se o CA =true o certificado pode assinar uma EC; Na ECR-CV CA= True
	cRLDistributionPoints	4.2.1.13	*http://pki.ecrcv.cv/pub/crl/ec_raiz_crl001.crl*		
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

9.9. EXTENSÕES DE CERTIFICADO DE EC SUBORDINADA

Componente do Certificado		Secção no RFC 3280	Valor	Tipo[23]	Comentários
tbsCertificate	**Version**	4.1.2.1	2	m	O valor 2 identifica a utilização de certificados ITU-T X.509 versão 3.
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"ANAC-Agencia Nacional das Comunicacoes"		
	Common Name (CN)		"Entidade de Certificacao Raiz de Cabo Verde 001"		
	Validity	4.1.2.5		m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralisedTime*
	Not Before		<data de emissão>		
	Not After		<data de emissão + 12 anos>		Validade de 12 anos com renovação a cada 6 anos.
	Subject	4.1.2.6	<O DN sera definido pela Entidade Subordinada>	m	

[23] O perfil utilize a terminologia seguinte para cada um dos tipos de campo no certificado X.509:
m – mandatório (o campo TEM que estar presente)
o – opcional (o campo PODE estar presente)
c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

Componente do Certificado		Secção no RFC 3280	Valor	Tipo	Comentários
	Country (C)		"CV"		
	Organization (O)		"ICP-CV"		
	Organization Unit (OU)		"EC"		
	Common Name (CN)		<A definir pela Entidade Subordinada>		
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman).
	Algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.[24]
	subjectPublicKey		<Chave Pública com modulus n de 4096 bits>		
	Unique Identifiers	4.1.2.8		m	O "*unique identifiers*" está presente para permitir a possibilidade de reutilizar os nomes do *subject* e/ou *issuer* 20
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		m	
	keyIdentifier		O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	

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

Componente do Certificado		Secção no RFC 3280	Valor	Tipo	Comentários
	Subject Key Identifier	4.2.1.2	O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA.
	Digital Signature		"0" seleccionado		
	Non Repudiation		"0" seleccionado		
	Key Encipherment		"0" seleccionado		
	Data Encipherment		"0" seleccionado		
	Key Agreement		"0" seleccionado		
	Key Certificate Signature		"1" seleccionado		
	CRL Signature		"1" seleccionado		
	Encipher Only		"0" seleccionado		
	Decipher Only		"0" seleccionado		
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		2.5.29.32.0	m	
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.ecrcv.cv/pub/pol/ec_raiz_dpc_001_pt.html	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Declaração de Práticas de Certificação publicada pela ECR-CV. O apontador está na forma de um URI."
	Basic Constraints	4.2.1.10		mc	Esta extensão é marcada CRÍTICA.

Componente do Certificado		Secção no RFC 3280	Valor	Tipo	Comentários
	CA		TRUE		Indica o tipo de Entidade a quem se destina o certificado; restrição básica, se o CA =true o certificado pode assinar uma EC
	PathLenConstraint		0		
	cRLDistributionPoints	4.2.1.13	*http://pki.ecrcv.cv/pub/crl/ec_raiz_crl001.crl*		
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

9.10. PERFIL DE LCR

9.9.1. 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.20

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

9.9.3. O perfil da LCR está de acordo com:

a) Recomendação ITU.T X.509[25];

b) RFC 5280;

c) Política de Certificados da ICP-CV[26].

9.11. NÚMERO(S) DE VERSÃO

A ECR-CV implementa a sua LCR conforme a versão 2 do padrão ITU X.509.

9.12. EXTENSÕES DE LCR DA ECR-CV

As componentes e as extensões definidas para as LCRs X.509 v2 fornecem métodos para associar atributos às LCRs.

Componente da LCR		Secção no RFC 5280	Valor	Tipo	Comentários
	Version	5.1.2.1	1	m	O valor 1 identifica a utilização da Versão 2 do padrão ITU X.509
	Signature	5.1.2.2	1.2.840.113549.1.1.11	m	Contém o identificador do algoritmo utilizado para assinar a LCR. O valor TEM que ser igual ao OID no campo *signatureAlgorithm* (abaixo)
	Issuer	5.1.2.3		m	
	Country (C)		”CV”		
	Organization (O)		“ICP-CV”		
	Common Name (CN)		“ Entidade de Certificacao Raiz de Cabo Verde ”		

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

[26] Infra-estrutura de Chave Pública de Cabo Verde

Componente da LCR		Secção no RFC 5280	Valor	Tipo	Comentários
	thisUpdate	5.1.2.4	<data de emissão da LCR>	m	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime.
	nextUpdate	5.1.2.5	<data da próxima emissão da LCR = *thisUpdate* + N>	m	Este campo indica a data em que a próxima LCR vai ser emitida. A próxima LCR pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da LCR DEVEM emitir LCR com o tempo de nextUpdate maior ou igual a todas as LCR anteriores. Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime. N será no máximo 90 dias.
	revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key Identifier	5.2.1		o	
	keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	
	CRL Number	5.2.3	<número sequencial único e incrementado>	m	
	CRL Entry Extensions	5.3			
	Reason Code	5.3.1		o	Valor tem que ser um dos seguintes: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold

Componente da LCR		Secção no RFC 5280	Valor	Tipo	Comentários
					8 – removeFromCRL 9 – privilegeWithdrawn 10 - aACompromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a *tbsCertList*.

9.13. PERFIL OCSP

Não aplicável.

10. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

10.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

10.1.1. A Administração de Segurança da ECR-CV determina a conformidade e aplicação interna desta DPC (e/ou respectivas PC's), submetendo-a ao Conselho Executivo da ECRCV que por sua vez, e após a sua aprovação, a submete ao CG – órgão competente para determinar a adequação da DPC (e/ou respectivas PC's) das diversas entidades, com a Política de Certificados definida pela ICP-CV – para aprovação.

10.1.2. A Administração de Segurança da ECR-CV é responsável pela constante actualização desta DPC garantindo que a mesma é revista pelo menos anualmente. Sempre que for registada necessidade de alterações as mesmas devem ser feitas pela Administração de Segurança, revistas pela Comissão executiva e aprovadas pelo CG da ICP-CV.

10.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

As actualizações a esta DPC serão publicadas imediatamente após a sua aprovação pelo CG, de acordo com a secção 10.12.

10.3. PROCEDIMENTOS PARA APROVAÇÃO

10.3.1. A aprovação interna desta DPC e seguintes correcções (ou actualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Administração de Segurança. Correcções (ou actualizações) deverão ser publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definida. O Grupo de Trabalho de Administração de Segurança deverá ainda determinar quando é que as alterações na DPC levam a uma alteração nos identificadores dos objectos (OID) da DPC.

10.3.2. Após a aprovação interna pelo conselho executivo, a DPC é submetida ao CG, que é a entidade responsável pela aprovação e autorização de modificações neste tipo de documentos.

10.4. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

10.4.1. TAXAS

10.4.1.1. Taxas por emissão ou renovação de certificados – de acordo com legislação em vigor.

10.4.1.2. Taxas para acesso a certificado - Nada a assinalar.

10.4.1.3. Taxas para acesso a informação do estado do certificado ou de revogação - livre e gratuita.

10.4.1.4. Taxas para outros serviços - Nada a assinalar.

10.4.1.5. Política de reembolso -Nada a assinalar.

10.5. RESPONSABILIDADE FINANCEIRA

10.5.1. SEGURO

10.5.1.1. Seguro de cobertura - Nada a assinalar.

10.5.1.2. Outros recursos - Nada a assinalar.

10.5.1.3. Seguro ou garantia de cobertura para utilizadores - Nada a assinalar.

10.6. CONFIDENCIALIDADE DA INFORMAÇÃO PROCESSADA

10.6.1. ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

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

a) As chaves privadas da ECR-CV;

b) As chaves privadas das entidades da ECR-CV;

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

d) Toda a informação de carácter pessoal proporcionada à ECR-CV durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;

e) Planos de continuidade de negócio e recuperação;

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

g) Informação de todos os documentos relacionados com a ECR-CV (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, constitui informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade da ANAC. Estes documentos são confiados aos recursos humanos dos Grupos de Trabalho da ECR-CV 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 ANAC;

h) Todas as palavras-chave, PINs e outros elementos de segurança relacionados com a ECR-CV;

i) A identificação dos membros dos grupos de trabalho da ECR-CV;

j) A localização dos ambientes da ECR-CV e seus conteúdos.

10.6.2. INFORMAÇÃO FORA DO ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

10.5.1.4. Considera-se informação de acesso público:

a) DPC;

b) LCR;

c) Toda a informação classificada como "pública".

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

10.6.3. RESPONSABILIDADE DE PROTECÇÃO DA CONFIDENCIALIDADE DA INFORMAÇÃO

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

10.7. PRIVACIDADE DOS DADOS PESSOAIS

10.7.1. MEDIDAS PARA GARANTIA DA PRIVACIDADE

10.7.1.1. Certificados pessoais - Nada a assinalar, dado que não são emitidos certificados pessoais sob a ECR-CV.

10.7.1.2. Informação privada - Nada a assinalar.

10.7.1.3. Informação não protegida pela privacidade - Nada a assinalar.

10.7.1.4. Responsabilidade de protecção da informação privada - Nada a assinalar.

10.7.1.5. Notificação e consentimento para utilização de informação privada - Nada a assinalar.

10.7.1.6. Divulgação resultante de processo judicial ou administrativo - Nada a assinalar.

10.7.1.7. Outras circunstâncias para revelação de informação - Nada a assinalar.

10.8. RENÚNCIA DE GARANTIAS

10.8.1. A ECR-CV recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

10.9. INDEMNIZAÇÕES

De acordo com a legislação em vigor

10.10. TERMO E CESSAÇÃO DA ACTIVIDADE

10.10.1. TERMO

10.10.1.1. Os documentos relacionados com a ECR-CV (incluindo esta DPC) tornam-se efectivos logo que sejam aprovados pelo CG e apenas são eliminados ou alterados por sua ordem.

10.10.1.2. Esta DPC entra em vigor desde o momento da sua publicação no repositório da ECR-CV.

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

10.10.2. SUBSTITUIÇÃO E REVOGAÇÃO DA DPC

10.10.2.1. O Conselho Executivo ou o CG podem decidir em favor da eliminação ou emenda de um documento relacionado com a ECR-CV (incluindo esta DPC) quando:

a) Os seus conteúdos são considerados incompletos, imprecisos ou erróneos;

b) Os seus conteúdos foram comprometidos.

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

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

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

10.10.3. CONSEQUÊNCIAS DA CESSAÇÃO DE ACTIVIDADE

10.10.3.1. Após o Conselho Executivo ou o CG decidir em favor da eliminação de um documento relacionado com a EC, o Grupo de Trabalho de Administração de Segurança tem 30 dias úteis para submeter para aprovação pelo Conselho Executivo e pelo CG um documento(s) substituto.

10.10.3.2. As obrigações e restrições estabelecidas nesta DPC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da ECR-CV, nascidas sob sua vigência, subsistirão após a sua substituição ou revogação por uma nova versão em tudo o que não se oponha a esta.

10.11. NOTIFICAÇÃO INDIVIDUAL E COMUNICAÇÃO AOS PARTICIPANTES

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

10.12. ALTERAÇÕES

10.12.1. PROCEDIMENTO PARA ALTERAÇÕES

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

a) A identificação da pessoa que submeteu o pedido de alteração;

b) A razão do pedido;

c) As alterações pedidas.

10.12.1.2. O Grupo de Trabalho de Administração de Segurança deve rever o pedido feito e, se verificar a sua pertinência, proceder às actualizações necessárias ao documento, resultando numa nova versão de rascunho do documento.

10.12.1.3. O novo rascunho do documento é depois disponibilizado a todos os membros do Grupo de Trabalho. 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 Administração de Segurança 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 pelo Conselho Executivo e fornecido ao CG para aprovação. Depois da sua aprovação, o documento é submetido para o Conselho Executivo para publicação, tornando-se as alterações finais e efectivas.

10.12.2. PRAZO E MECANISMO DE NOTIFICAÇÃO

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

10.12.3. MOTIVOS PARA MUDANÇA DE OID

No caso em que o Grupo de Trabalho de Administração de Segurança julgue que as alterações à especificação podem afectar a aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objecto (OID) que o representa.

10.13. DISPOSIÇÕES PARA RESOLUÇÃO DE CONFLITOS

10.13.1. Todos os conflitos entre utilizadores e a ECR-CV deverão ser comunicados pela parte em disputa à ANAC, com o fim de tentar resolvê-lo entre as mesmas partes.

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

10.14. LEGISLAÇÃO APLICÁVEL

É aplicável à actividade das Entidades de Certificação a seguinte legislação específica:

a) Decreto-Lei nº 33 /2007, de 24 de Setembro;

b) Decreto-Lei nº44/2009 de 9 de Novembro;

c) Portaria nº 2/2008, de 28 de Janeiro;

d) Portaria Conjunta nº 4/2008, de Fevereiro de 2008;

e) Decreto Regulamentar nº. 18/2007, de 24 de Dezembro.

10.15. CONFORMIDADE COM A LEGISLAÇÃO EM VIGOR

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

10.16.2. É responsabilidade do CG zelar pelo cumprimento da legislação aplicável listada na secção 10.144.

10.16. PROVIDÊNCIAS VÁRIAS

10.16.1. ACORDO COMPLETO

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

10.16.2. INDEPENDÊNCIA

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

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

10.16.3. SEVERIDADE

Nada a assinalar.

10.16.4. EXECUÇÕES (TAXAS DE ADVOGADOS E DESISTÊNCIA DE DIREITOS)

Nada a assinalar.

10.16.5. FORÇA MAIOR

Nada a assinalar.

10.16.6. OUTRAS PROVIDÊNCIAS

Nada a assinalar.

Referências Bibliográficas

[1] ANAC, Estrutura da Declaração de Práticas de Certificação.
[2] ANAC, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança.

[3] Portaria nº 2/2008, de 28 de Janeiro;

[4] Decreto-Lei nº44/2009 de 9 de Novembro;

[5] Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;

[6] Decreto-Lei nº 33 /2007, de 24 de Setembro;

[7] Portaria nº 4/2008

[8] FIPS 140-2. 1994, Security Requirements for Cryptographic Modules.

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

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

[11] 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.

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

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

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

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

[16] RFC 2252. 1997, Lightweight Directory Access Protocol (v3).

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

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

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

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

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

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

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

[24] Política de Certificado da EC Raiz de Cabo Verde