



**POLÍTICA DE CERTIFICADOS DA SCEE**  
**e**  
**Requisitos mínimos de Segurança**

**Versão 1.0, de 14 de Julho de 2006**

**OID: 2.16.620.1.1.1.2.1.1.0**

# ÍNDICE

1. INTRODUÇÃO.....	11
1.1. Enquadramento.....	11
1.1.1. Âmbito.....	11
1.1.2. Estrutura do documento.....	11
1.1.3. Hierarquia de OiD da SCEE.....	12
1.2. Identificação do documento.....	12
1.3. Participantes na Infra-estrutura de Chaves Públicas.....	13
1.3.1. Entidades Certificadoras (EC).....	13
1.3.2. Entidades de Registo (ER).....	15
1.3.3. Titulares de Certificados.....	15
1.3.4. Partes confiantes.....	16
1.3.5. Outros participantes.....	16
1.4. Utilização do certificado.....	18
1.4.1. Utilização adequada.....	18
1.4.2. Utilização não autorizada.....	19
1.5. Gestão das políticas.....	19
1.5.1. Entidade responsável pela Gestão do documento.....	19
1.5.2. Contacto.....	19
1.5.3. Entidade que determina a conformidade da Declaração de Práticas de Certificação (DPC) para a Política.....	20
1.5.4. Procedimentos para aprovação da DPC.....	20
1.6. Definições e acrónimos.....	20
2. RESPONSABILIDADE DE PUBLICAÇÃO E REPOSITÓRIO.....	21
2.1. Repositórios.....	21
2.2. Publicação de informação de certificação.....	21
2.3. Periodicidade de publicação.....	22
2.4. Controlo de acesso aos repositórios.....	22
3. IDENTIFICAÇÃO E AUTENTICAÇÃO.....	23
3.1. Atribuição de nomes.....	23
3.1.1. Tipo de nomes.....	23
3.1.2. Necessidade de nomes significativos.....	24
3.1.3. Anonimato ou pseudónimo de titulares.....	24
3.1.4. Interpretação de formato de nomes.....	24
3.1.5. Unicidade de nomes.....	24
3.1.6. Reconhecimento, autenticação e funções das marcas registadas.....	25

3.2. Validação de identidade no registo inicial.....	25
3.2.1. Método de comprovação da posse de chave privada.....	25
3.2.2. Autenticação da identidade de uma pessoa colectiva.....	25
3.2.3. Autenticação da identidade de uma pessoa singular.....	26
3.2.4. Informação de subscritor/titular não verificada.....	27
3.2.5. Critérios para interoperabilidade.....	28
3.3. Identificação e autenticação para pedidos de renovação de chaves.....	28
3.3.1. Identificação e autenticação para renovação de chaves, de rotina.....	28
3.3.2. Identificação e autenticação para renovação de chaves, após revogação.....	28
3.4. Identificação e autenticação para pedido de revogação.....	28
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO.....	30
4.1. Pedido de certificado.....	30
4.1.1. Quem pode subscrever um pedido de certificado.....	30
4.1.2. Processo de registo e responsabilidades.....	30
4.2. Processamento do pedido de certificado.....	30
4.2.1. Processos para a identificação e funções de autenticação.....	30
4.2.2. Aprovação ou recusa de pedidos de certificado.....	31
4.2.3. Prazo para processar o pedido de certificado.....	31
4.3. Emissão de certificado.....	31
4.3.1. Procedimentos para a emissão de certificado.....	31
4.3.2. Notificação da emissão do certificado ao titular.....	32
4.4. Aceitação do certificado.....	32
4.4.1. Procedimentos para a aceitação de certificado.....	32
4.4.2. Publicação do certificado.....	32
4.4.3. Notificação da emissão de certificado a outras entidades.....	33
4.5. Uso do certificado e par de chaves.....	33
4.5.1. Uso do certificado e da chave privada pelo titular.....	33
4.5.2. Uso do certificado e da chave pública pelas partes confiantes.....	34
4.6. Renovação de certificados.....	34
4.6.1. Motivos para renovação de certificado.....	34
4.6.2. Quem pode submeter o pedido de renovação de certificado.....	34
4.6.3. Processamento do pedido de renovação de certificado.....	34
4.6.4. Notificação de emissão de novo certificado ao titular.....	34
4.6.5. Procedimentos para aceitação de certificado.....	35
4.6.6. Publicação de certificado após renovação.....	35
4.6.7. Notificação da emissão do certificado a outras entidades.....	35
4.7. Renovação de certificado com geração de novo par de chaves.....	35

4.7.1. Motivos para a renovação de certificado com geração de novo par de chaves	35
4.7.2. Quem pode submeter o pedido de certificação de uma nova chave pública....	35
4.7.3. Processamento do pedido de renovação de certificado com geração de novo par de chaves .....	35
4.7.4. Notificação da emissão de novo certificado ao titular.....	36
4.7.5. Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves.....	36
4.7.6. Publicação de novo certificado renovado com geração de novo par de chaves .....	36
4.7.7. Notificação da emissão de novo certificado a outras entidades.....	36
4.8. Modificação de certificados.....	36
4.8.1. Motivos para alteração de certificado .....	36
4.8.2. Quem pode submeter o pedido de alteração de certificado.....	36
4.8.3. Processamento do pedido de alteração de certificado .....	36
4.8.4. Notificação da emissão de certificado alterado ao titular .....	37
4.8.5. Procedimentos para aceitação de certificado alterado.....	37
4.8.6. Publicação do certificado alterado .....	37
4.8.7. Notificação da emissão de certificado alterado a outras entidades.....	37
4.9. Suspensão e revogação de certificado.....	37
4.9.1. Motivos para a revogação .....	37
4.9.2. Quem pode submeter o pedido de revogação .....	38
4.9.3. Procedimento para o pedido de revogação .....	38
4.9.4. Produção de efeitos da revogação .....	39
4.9.5. Prazo para processar o pedido de revogação.....	39
4.9.6. Requisitos de verificação da revogação pelas parte confiantes.....	39
4.9.7. Periodicidade da emissão da Lista de Certificados Revogados (LCR) .....	39
4.9.8. Período máximo entre a emissão e a publicação da CRL.....	39
4.9.9. Disponibilidade de verificação on-line do estado / revogação de certificado.....	40
4.9.10. Requisitos de verificação on-line de revogação.....	40
4.9.11. Outras formas disponíveis para divulgação de revogação.....	40
4.9.12. Requisitos especiais em caso de comprometimento de chave privada.....	40
4.9.13. Motivos para suspensão.....	40
4.9.14. Quem pode submeter o pedido de suspensão .....	40
4.9.15. Procedimentos para pedido de suspensão .....	40
4.9.16. Limite do período de suspensão.....	40
4.10. Serviços sobre o estado do certificado.....	40
4.10.1. Características operacionais.....	40

4.10.2. Disponibilidade de serviço .....	41
4.10.3. Características opcionais .....	41
4.11. Fim de subscrição.....	41
4.12. Retenção e recuperação de chaves ( <i>key escrow</i> ).....	41
4.12.1. Políticas e práticas de recuperação de chaves .....	41
4.12.2. Políticas e práticas de encapsulamento e recuperação de chaves de sessão....	41
5. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS.....	42
5.1. Medidas de segurança física.....	42
5.1.1. Localização física e tipo de construção.....	42
5.1.2. Acesso físico ao local .....	42
5.1.3. Energia e ar condicionado.....	43
5.1.4. Exposição à água.....	43
5.1.5. Prevenção e protecção contra incêndio.....	43
5.1.6. Salvaguarda de suportes de armazenamento .....	43
5.1.7. Eliminação de resíduos.....	43
5.1.8. Instalações externas (alternativa) para recuperação de segurança .....	44
5.2. Medidas de segurança dos processos .....	44
5.2.1. Funções de confiança.....	44
5.2.2. Número de pessoas exigidas por tarefa.....	45
5.2.3. Identificação e autenticação para cada função .....	45
5.2.4. Funções que requerem separação de responsabilidades.....	46
5.3. Medidas de segurança de pessoal .....	46
5.3.1. Requisitos relativos às qualificações, experiência, antecedentes e credenciação	47
5.3.2. Procedimentos de verificação de antecedentes.....	47
5.3.3. Requisitos de formação e treino.....	47
5.3.4. Frequência e requisitos para acções de reciclagem.....	48
5.3.5. Frequência e sequência da rotação de funções.....	48
5.3.6. Sanções para acções não autorizadas.....	48
5.3.7. Contratação de pessoal.....	48
5.3.8. Documentação fornecida ao pessoal.....	48
5.4. Procedimentos de auditoria de segurança .....	49
5.4.1. Tipo de eventos registados.....	49
5.4.2. Frequência da auditoria de registos.....	49
5.4.3. Período de retenção dos registos de auditoria .....	49
5.4.4. Protecção dos registos de auditoria .....	50
5.4.5. Procedimentos para a cópia de segurança dos registos .....	50
5.4.6. Sistema de recolha de dados de auditoria (interno/externo).....	50

5.4.7. Notificação de agentes causadores de eventos.....	50
5.4.8. Avaliação de vulnerabilidades.....	50
5.5. Arquivo de registos.....	51
5.5.1. Tipo de dados arquivados.....	51
5.5.2. Período de retenção em arquivo.....	51
5.5.3. Protecção dos arquivos.....	51
5.5.4. Procedimentos para as cópias de segurança do arquivo.....	51
5.5.5. Requisitos para validação cronológica dos registos.....	51
5.5.6. Sistema de recolha de dados de arquivo (interno/externo).....	51
5.5.7. Procedimentos de recuperação e verificação de informação arquivada.....	52
5.6. Renovação de chaves.....	52
5.7. Recuperação em caso de desastre ou comprometimento.....	52
5.7.1. Procedimentos em caso de incidente ou comprometimento.....	52
5.7.2. Corrupção dos recursos informáticos, do software e/ou dos dados.....	52
5.7.3. Procedimentos em caso de comprometimento da chave privada da entidade.....	53
5.7.4. Capacidade de continuidade da actividade em caso de desastre.....	54
5.8. Procedimentos em caso de extinção de EC ou ER.....	54
6. MEDIDAS DE SEGURANÇA TÉCNICAS.....	55
6.1. Geração e instalação do par de chaves.....	55
6.1.1. Geração do par de chaves.....	55
6.1.2. Entrega da chave privada ao titular.....	56
6.1.3. Entrega da chave pública ao emissor do certificado.....	56
6.1.4. Entrega da chave pública da EC às partes confiantes.....	56
6.1.5. Dimensão das chaves.....	56
6.1.6. Geração dos parâmetros da chave pública e verificação da qualidade.....	57
6.1.7. Fins a que se destinam as chaves (campo “key usage” X.509v3).....	57
6.1.8. Outra utilização para as chaves.....	58
6.2. Protecção da chave privada e características do módulo criptográfico.....	58
6.2.1. Normas e medidas de segurança do módulo criptográfico.....	59
6.2.2. Controlo multi-pessoal (N de M) para a chave privada.....	59
6.2.3. Retenção da chave privada (key escrow).....	59
6.2.4. Cópia de segurança da chave privada.....	59
6.2.5. Arquivo da chave privada.....	60
6.2.6. Transferência da chave privada para/do módulo criptográfico.....	60
6.2.7. Armazenamento da chave privada no módulo criptográfico.....	60
6.2.8. Processo para activação da chave privada.....	60
6.2.9. Processo para desactivação da chave privada.....	60

6.2.10. Processo para destruição da chave privada.....	61
6.2.11. Avaliação/nível do módulo criptográfico.....	61
6.3. Outros aspectos da gestão do par de chaves.....	61
6.3.1. Arquivo da chave pública.....	61
6.3.2. Períodos de validade do certificado e das chaves.....	62
6.4. Dados de activação.....	62
6.4.1. Geração e instalação dos dados de activação.....	62
6.4.2. Protecção dos dados de activação.....	62
6.4.3. Outros aspectos dos dados de activação.....	63
6.5. Medidas de segurança informática.....	63
6.5.1. Requisitos técnicos específicos.....	63
6.5.2. Avaliação/nível de segurança.....	63
6.6. Ciclo de vida das medidas técnicas de segurança.....	64
6.6.1. Medidas de desenvolvimento do sistema.....	64
6.6.2. Medidas para a gestão da segurança.....	64
6.6.3. Ciclo de vida das medidas de segurança.....	65
6.7. Medidas de segurança da rede.....	65
6.8. Validação cronológica (Time-stamping).....	65
7. PERFIS DE CERTIFICADO, CRL E OCSP.....	67
7.1. Perfil do certificado.....	67
7.1.1. Número(s) de versão.....	67
7.1.2. Extensões do certificado.....	67
7.1.3. Identificadores de algoritmo.....	68
7.1.4. Formatos de nome.....	69
7.1.5. Restrições de nome.....	69
7.1.6. Objecto identificador da política de certificado.....	69
7.1.7. Utilização da extensão de restrição de políticas.....	69
7.1.8. Sintaxe e semântica dos qualificadores de políticas.....	69
7.1.9. Semântica de processamento da extensão de política de certificados críticos.....	69
7.2. Perfil da LCR.....	70
7.2.1. Número(s) da versão.....	70
7.2.2. Extensões da CRL e das suas entradas.....	71
7.3. Perfil do OCSP.....	71
7.3.1. Número(s) da versão.....	71
7.3.2. Extensões do OCSP.....	71
8. AUDITORIA E AVALIAÇÕES DE CONFORMIDADE.....	73
8.1. Frequência ou motivo da auditoria.....	73

8.2. Identidade e qualificações do auditor.....	73
8.3. Relação entre o auditor e a entidade certificadora.....	73
8.4. Âmbito da auditoria.....	74
8.5. Procedimentos após uma auditoria com resultado deficiente.....	74
8.6. Comunicação de resultados.....	75
9. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS.....	76
9.1. Taxas.....	76
9.1.1. Taxas por emissão ou renovação de certificados.....	76
9.1.2. Taxas para acesso a certificado.....	76
9.1.3. Taxas para acesso a informação do estado certificado ou de revogação.....	76
9.1.4. Taxas para outros serviços.....	76
9.1.5. Política de reembolso.....	76
9.2. Responsabilidade financeira.....	76
9.2.1. Seguro de cobertura.....	76
9.2.2. Outros recursos.....	76
9.2.3. Seguro ou garantia de cobertura para utilizadores.....	77
9.3. Confidencialidade da informação processada.....	77
9.3.1. Âmbito da confidencialidade da informação.....	77
9.3.2. Informação fora do âmbito da confidencialidade da informação.....	77
9.3.3. Responsabilidade de protecção da confidencialidade da informação.....	77
9.4. Privacidade dos dados pessoais.....	78
9.4.1. Medidas para garantia da privacidade.....	78
9.4.2. Informação privada.....	78
9.4.3. Informação não protegida pela privacidade.....	79
9.4.4. Responsabilidade de protecção da informação privada.....	79
9.4.5. Notificação e consentimento para utilização de informação privada.....	79
9.4.6. Divulgação resultante de processo judicial ou administrativo.....	79
9.4.7. Outras circunstâncias para revelação de informação.....	79
9.5. Direitos de propriedade intelectual.....	80
9.6. Representações e garantias.....	80
9.6.1. Representação e garantias das Entidades Certificadoras.....	80
9.6.2. Representação e garantias das Entidades de Registo.....	81
9.6.3. Representação e garantias dos titulares.....	82
9.6.4. Representação e garantias das partes confiantes.....	83
9.6.5. Representação e garantias de outros participantes.....	83
9.7. Renúncia de garantias.....	83
9.8. Limitações às obrigações.....	83

9.9. Indemnizações .....	84
9.10. Termo e cessação da actividade .....	84
9.10.1. Termo .....	84
9.10.2. Substituição e revogação da PC.....	84
9.10.3. Consequências da cessação da actividade.....	85
9.11. Notificação individual e comunicação aos participantes .....	85
9.12. Alterações .....	85
9.12.1. Procedimento para alterações .....	85
9.12.2. Prazo e mecanismo de notificação .....	85
9.12.3. Motivos para mudar de OID.....	85
9.13. Disposições para resolução de conflitos.....	86
9.14. Legislação aplicável .....	86
9.15. Conformidade com a legislação em vigor .....	86
9.16. Providências várias.....	86
9.16.1. Acordo completo .....	86
9.16.2. Independência.....	87
9.16.3. Severidade .....	87
9.16.4. Execuções (taxas de advogados e desistência de direitos) .....	87
9.16.5. Força maior .....	87
9.17. Outras providências .....	87
A. Anexo - PERFIL DOS CERTIFICADOS.....	88
A.1. Perfil de Certificado de ECRaizEstado.....	88
A.2. Perfil de Certificado de ECEstado.....	90
A.3. Perfil de Certificado de Assinatura Digital .....	92
A.4. Perfil de Certificado de Autenticação.....	94
A.5. Perfil de Certificado de Confidencialidade.....	96
B. Anexo – PERFIL DAS LCR .....	98
C. Anexo – NORMALIZAÇÃO TÉCNICA .....	99
D. Anexo – DEFINIÇÕES E ACRÓNIMOS.....	112
D.1. Acrónimos .....	112
D.2. Definições.....	114
E. Anexo – Hierarquia de OID da SCEE .....	119

## ÍNDICE DE TABELAS

Tabela 1 - Hierarquia superior de OID.....	12
Tabela 2 – Dados relativos à Política de certificados da SCEE .....	13
Tabela 3 - Dados dos certificados da ECRaizEstado .....	14
Tabela 4 – Perfis de certificados suportados pela SCEE .....	18
Tabela 5 – Dados para contacto .....	20
Tabela 6 – Prazos mínimos para renovação da informação pelas diversas entidades .....	22
Tabela 7 – Regras para o preenchimento do DN.....	24
Tabela 8 – Incompatibilidade entre funções .....	46
Tabela 9 – Credenciação de segurança .....	47
Tabela 10 – Procedimentos em caso de comprometimento de chaves.....	53
Tabela 11 – Definição dos campos “Keyusage” dos Certificados SCEE .....	57
Tabela 12 – Definição dos Períodos de Validade dos Certificados .....	62
Tabela 13 – Campos básicos do certificado.....	67
Tabela 14 – Identificadores OiD de Algoritmos .....	68
Tabela 15– Campos básicos do certificado .....	70
Tabela 16 – Prazos de comunicação dos resultados de Auditoria .....	75

---

# 1. INTRODUÇÃO

---

---

## 1.1. ENQUADRAMENTO

---

---

### 1.1.1. ÂMBITO

---

Decorrente da implementação em curso 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 através da Resolução do Conselho de Ministros n.º 171/2005, publicada em D.R. em 3 de Novembro de 2005, a criação da Sistema de Certificação Electrónica do Estado (SCEE) – Infra-estrutura de Chaves Públicas. Esses programas envolvem, para certos fins específicos, mecanismos de autenticação digital forte de identidades e assinaturas electrónicas que podem ser concretizados mediante a utilização das denominadas infra-estruturas de chaves públicas.

São exemplos de projectos programados ou em curso no âmbito da sociedade da informação e do governo electrónico os relativos ao cartão do cidadão, ao passaporte electrónico português, à certificação electrónica do Governo e à disponibilização de serviços da Administração Pública pela Internet que requeiram autenticação digital forte de identidades e assinaturas electrónicas e à desmaterialização dos processos intra e inter-organismos do Estado que requeiram esse tipo de autenticação.

A arquitectura do SCEE constituirá assim uma hierarquia de confiança, que promoverá a segurança electrónica do Estado.

Para o efeito a SCEE compreenderá um Conselho Gestor que dá parecer sobre a aprovação e integração de entidades certificadoras no SCEE pronunciando-se igualmente sobre práticas e políticas de certificação, uma Entidade Certificadora Electrónica Raiz, que constitui o primeiro nível da cadeia hierárquica de certificação, e as várias Entidades Certificadoras do Estado a esta subordinadas.

Esta entidade deve funcionar independentemente de outras infra-estruturas de chaves públicas de natureza privada ou estrangeira, mas deve permitir a interoperabilidade com as infra-estruturas que satisfaçam os requisitos necessários de rigor de autenticação, através dos mecanismos técnicos adequados, e da compatibilidade em termos de políticas de certificação, nomeadamente no âmbito dos países da União Europeia (UE).

Assim, é criada a Sistema de Certificação Electrónica do Estado Português – Infra-Estrutura de Chaves Públicas, adiante designada como SCEE, que opera para os organismos e funcionários da Administração Pública bem como para as pessoas singulares e colectivas no seu relacionamento com o Estado. A SCEE estabelece uma estrutura de confiança electrónica, de forma a que os serviços disponibilizados pelas entidades certificadoras que a compõem, proporcionem nomeadamente a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

---

### 1.1.2. ESTRUTURA DO DOCUMENTO

---

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infra-estruturas de chave pública e assinatura electrónica. Caso esta situação não se verifique recomenda-se o

aprofundar de conceitos e conhecimento nos tópicos anteriormente focado antes de proceder com a leitura do documento.

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF, no documento RFC 3647.

De forma a facilitar a leitura e consequente análise deste documentos com as práticas difundidas e recomendadas internacionalmente, optou-se por incluir todas a secções estabelecidas no índice do documento supracitado, pelo que se não houver nada designado sobre o assunto, será incluída a expressão “nada a assinalar”.

Ainda de acordo com este pressuposto foi tido em consideração as especificações e recomendações definidas nos vários documentos emanados pelo PKIX *Working Group*, União Europeia e pela legislação nacional aplicável.

---

### 1.1.3. HIERARQUIA DE OID DA SCEE

---

Os OID são identificadores utilizados para referenciar objectos de forma inequívoca num determinado contexto, neste caso, a SCEE, funcionando por hierarquias. Neste particular a união “ISO-ITU-T” é a responsável pela atribuição de OID para os países.

A SCEE tem referenciado, mas não atribuído oficialmente, o OID = 2.16.620.1.1, com base na seguinte referência superior:

1	Estado Português
620	Portugal
16	Country assignments
2	ISO/ITU-T jointly assigned OIDs

Tabela 1 - Hierarquia superior de OID

#### 1.1.3.1. Distribuição da árvore 2.16.620.1.1 {id-scee}

---

No âmbito da infra-estrutura de chave pública da SCEE, a distribuição dos OID, tendo em consideração a necessidade de atribuição de identificadores aos objectos digitais de toda a infra-estrutura (documentos, extensões e perfis de certificados, e outras extensões do protocolo PKIX), será feita tendo em conta a hierarquia global definida no Anexo X.

---

## 1.2. IDENTIFICAÇÃO DO DOCUMENTO

---

Em virtude dos vários projectos em curso e tendo conta a diversidade e especificidade de cada um dos mesmos, as várias políticas de certificados são identificadas por um OiD, que

traduz a sua aplicabilidade na atribuição de certificados digitais por cada uma das Entidade Certificadoras do Estado. Os diversos OiD, estão de acordo com as especificações definidas na Estrutura de OID da SCEE, descrita anteriormente

Este documento de Política de Certificação é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 0.1
Estado do Documento	Em aprovação
OID	2.16.620.1.1.1.2.1.1.0
Data de Emissão	21 de Abril de 2006
Válidade	Não aplicável
Localização	<a href="http://www.scee.gov.pt/pcert">http://www.scee.gov.pt/pcert</a>

Tabela 2 – Dados relativos à Política de certificados da SCEE

### 1.3. PARTICIPANTES NA INFRA-ESTRUTURA DE CHAVES PÚBLICAS

#### 1.3.1. ENTIDADES CERTIFICADORAS (EC)

São entidades que, após devida autorização da Entidade de Certificação Electrónica do Estado (ECEE), estão habilitadas para criar, assinar, atribuir e gerir certificados. Na prática uma EC é composta pelo conjunto de equipamentos, aplicações, pessoal e procedimentos que são indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir a adequada gestão do ciclo de vida dos certificados descritos neste documento.

A hierarquia de confiança do SCEE compreende a Entidade Certificadora Raiz do Estado (ECRaizEstado), as Entidades Certificadoras do Estado (ECEstado) e Entidades Certificadoras Subordinadas (subECEstado).

As Entidades Certificadoras que compõem a SCEE são:

##### 1.3.1.1. A Entidade Certificadora Raiz do Estado

A Entidade Certificadora Raiz do Estado (ECEE) é a entidade certificadora de topo da cadeia de certificação da SCEE, executora das políticas de certificados e directrizes aprovadas pelo Conselho Gestor do SCEE. Compete a esta prestar os serviços de certificação às Entidades Certificadoras do Estado no nível hierárquico imediatamente inferior ao seu na cadeia de certificação em conformidade com as normas aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados digitais qualificados.

Os serviços de certificação digital disponibilizados pela Entidade de Certificação Raiz do Estado englobam exclusivamente: o processo de registo das entidades certificadoras, geração de certificados e gestão do seu ciclo de vida, disseminação dos certificados, das políticas e das práticas de certificação, a gestão de revogações e disponibilização do estado/situação das mesmas.

A definição do detalhe, composição e funcionamento estão definidos em documentação e legislação própria.

O quadro seguinte apresenta os dados mais relevantes relativos aos certificados da ECRaizEstado, sendo de destacar a adopção emissão de dois certificados (pkcs1-sha1WithRSAEncryption<sup>1</sup> e Certificado pkcs1-sha256WithRSAEncryption) para o mesmo par de chaves.

DN	CN= ECRAIZESTADO; O=SCEE; C=PT
Certificado pkcs1-sha1WithRSAEncryption	
Número de série	
Período de validade	
Impressão digital	
Certificado pkcs1-sha256WithRSAEncryption	
Número de série	
Período de validade	
Impressão digital	

Tabela 3 - Dados dos certificados da ECRaizEstado

A ECRaizEstado, é a Entidade Certificadora de primeiro nível. A sua função é estabelecer a raiz da cadeia de confiança da infra-estrutura de chaves públicas (PKI). Esta EC não emite certificados para utilizadores finais, emitindo apenas certificados para assinar as Entidades Certificadoras do Estado. A ECRaizEstado assina-se a si própria.

### 1.3.1.2. Entidades Certificadoras do Estado (ECEstado)

As ECEstado, são entidades que se encontram no nível imediatamente abaixo da ECRaizEstado, sendo a sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores. O seu certificado é assinado pela ECRaizEstado.

<sup>1</sup> O certificado pkcs1-sha1WithRSAEncryption é apenas publicado para efeitos de garantia de interoperabilidade, de modo a permitir que os sistemas e aplicações que não suportem o algoritmo pkcs1-sha256WithRSAEncryption, estejam habilitados para construir o caminho de certificação para validação de certificados e assinatura.

### **1.3.1.3. Entidades Certificadoras Subordinadas (subECEstado)**

---

As subECEstado, são entidades que se encontram no nível imediatamente abaixo das EC, tendo como função a prestação de serviços de certificação para o utilizador final. O seu certificado é assinado pela respectiva ECEstado.

### **1.3.2. ENTIDADES DE REGISTO (ER)**

---

São entidades que por via do estabelecimento de um acordo com uma Entidade Certificadora do Estado, estas delegam a prestação de serviços de identificação e registo de utilizadores, bem como a gestão de pedidos de revogação de certificados.

As Entidades de Registo desenvolvem a sua actividade de acordo com o estabelecido na DPC da respectiva EC e pela EGPC.

### **1.3.3. TITULARES DE CERTIFICADOS**

---

#### **1.3.3.1. Titulares**

---

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados por uma ECEstado ou subECEstado.

No âmbito do SCEE são considerados como titulares, aqueles em que o nome está inscrito no campo *Subject* do certificado e utilizam o certificado e respectiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descritas neste documento, sendo consideradas as seguintes categorias titulares:

- a) Pessoa singular;
- b) Pessoa colectiva;
- c) Equipamentos tecnológicos.

Não são considerados titulares, no âmbito deste documento, as seguintes categorias:

- a) Entidade Certificadoras, independentemente do nível a que se encontram;
- b) Entidades de Registo;
- c) O pessoal das Entidades Certificadoras e Entidades de Registo cujos certificados tem como uso exclusivo a operação dos respectivos sistemas.

#### **1.3.3.2. Patrocinador**

---

A emissão de certificados para equipamentos tecnológicos (p.e: computadores, firewall, routers, servidores, etc.) deve ser efectuada sempre sob responsabilidade humana, sendo esta entidade designada por patrocinador.

O patrocinador aceita o certificado e é responsável pela sua correcta utilização, bem como pela protecção e salvaguarda da sua chave privada.

---

### 1.3.4. PARTES CONFIANTES

---

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

Na prática, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado, podendo ser titular de certificados da comunidade SCEE ou não.

---

### 1.3.5. OUTROS PARTICIPANTES

---

#### 1.3.5.1. O Conselho Gestor do Sistema de Certificação Electrónico do Estado

---

O Conselho Gestor do SCEE é a entidade a quem cabe pronunciar-se sobre as políticas e práticas de certificação das entidades certificadoras que integram a SCEE.

Compete especialmente ao Conselho Gestor do SCEE:

- a) Definir, de acordo com a lei e tendo em conta as normas ou especificações internacionalmente reconhecidas, a política de certificação e as práticas de certificação a observar pelas entidades certificadoras que integram o SCEE;
- b) Garantir que as declarações de práticas de certificação das várias entidades certificadoras do Estado, bem como da entidade certificadora raiz do Estado, estão em conformidade com a política de certificação do SCEE;
- c) Propor os critérios para aprovação das entidades certificadoras que pretendam integrar o SCEE;
- d) Aferir a conformidade dos procedimentos seguidos pelas entidades certificadoras do Estado com as políticas e práticas aprovadas, sem prejuízo das competências legalmente cometidas à autoridade credenciadora;
- e) Pronunciar-se pela exclusão do SCEE das entidades certificadoras do Estado em caso de não conformidade com as políticas e práticas aprovadas, comunicando tal facto à autoridade credenciadora;
- f) Pronunciar-se sobre as melhores práticas internacionais no exercício das actividades de certificação electrónica e propor a sua aplicação;
- g) Representar institucionalmente o SCEE;

Compete, ainda, ao Conselho Gestor do SCEE a promoção das actividades necessárias para o estabelecimento de acordos de interoperabilidade, com base em certificação

cruzada, com outras infra-estruturas de chaves públicas, de natureza privada ou pública, nacionais ou internacionais, nomeadamente:

- a) Dar indicações à entidade certificadora raiz do Estado para a atribuição e a revogação de certificados emitidos com base em certificação cruzada;
- b) Definir os termos e condições para o início, a suspensão ou a finalização dos procedimentos de interoperabilidade com outras infra-estruturas de chaves públicas

A definição do detalhe, composição e funcionamento estão definidos em documentação e legislação própria.

### **1.3.5.2. Autoridade Credenciadora**

---

De uma forma geral o papel da Autoridade Credenciadora, no domínio da SCEE, está relacionado com a disponibilização de serviços de auditoria/inspeção de conformidade, no sentido de aferir se os processos utilizados pelas EC nas suas actividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos neste documento e com o estabelecido na DPC da respectiva entidade.

Assim, consideram-se como principais atribuições as seguintes:

- a) a condução de auditorias;
- b) a gestão do controlo de qualidade de todo o processo de certificação;
- c) a fixação da procedimentos e documentação relativa às auditorias;
- d) Gestão dos relatórios de auditoria, nomeadamente, na elaboração e recepção (quando efectuados por pessoal externo);
- e) a fixação de planos de medidas correctivas aplicáveis às entidades certificadoras da SCEE;
- f) a fixação e acompanhamento de metas para indicadores de qualidade que deverá propor para aprovação do Conselho Gestor do SCEE no contexto de objectivos estratégicos previamente fixados pelo Conselho Gestor do SCEE;
- g) a gestão da bolsa de auditores;
- h) a apresentação à ECEE de proposta de registo e de rescisão de registo de entidades certificadoras na SCEE;
- i) a promoção da competência técnica dos auditores.

### **1.3.5.3. Autoridades de Validação**

---

As Autoridades de Validação (AV), tem como função comprovar o estado dos certificados emitidos, através da utilização do protocolo *Online Certificate Status Protocol* (OCSP), de

forma a determinar o estado actual do certificado a pedido de uma entidade sem necessidade de recorrer à verificação do estado através da consulta das LCR.

### 1.4. UTILIZAÇÃO DO CERTIFICADO

Os certificados emitidos no domínio do SCEE são utilizados, pelos diversos os sistemas, aplicações, mecanismos e protocolos, com o objectivo de garantir os seguintes serviços de segurança:

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

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

Esta política engloba tipos e perfis de certificados, descritos sumariamente no quadro seguinte:

TIPO DE UTILIZAÇÃO	IDENTIFICADOR	OID	DESCRIÇÃO
Assinatura de Certificados e LCR	anyPolicy	2.5.29.32.0	ver Anexo A
Assinatura electrónica	scee-assinatura	2.16.620.1.1.1.2.10	
Autenticação	scee-autenticacao	2.16.620.1.1.1.2.20	
Confidencialidade	scee-confidencialidade	2.16.620.1.1.1.2.30	

Tabela 4 – Perfis de certificados suportados pela SCEE

#### 1.4.1. UTILIZAÇÃO ADEQUADA

Os requisitos e regras definidos neste documento, aplicam-se a todos os certificados emitidos pelas ECEstado e subECEstado que forem constituídas como parte integrante do domínio da SCEE.

Os certificados atribuídos a pessoas, singulares e colectivas, têm como objectivo a sua utilização em qualquer aplicação para efeitos de Assinatura digital, autenticação de cliente e encriptação.

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

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

Os certificados emitidos pela SCEE devem ser utilizados de acordo com a função e finalidade estabelecida nas Declaração de Práticas de Certificação e nas correspondentes Políticas de Certificados e de acordo com a lei em vigor.

---

### 1.4.2. UTILIZAÇÃO NÃO AUTORIZADA

---

Os certificados emitidos para os titulares não podem ser utilizados para desempenhar actividades como certificados de EC nem ER, conseqüentemente, não podem ser utilizados para assinar certificados nem LCR.

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

---

## 1.5. GESTÃO DAS POLÍTICAS

---

---

### 1.5.1. ENTIDADE RESPONSÁVEL PELA GESTÃO DO DOCUMENTO

---

A gestão desta política de certificados é da responsabilidade do Conselho Gestor.

---

### 1.5.2. CONTACTO

---

Nas DPC, devem ser incluídos, no mínimo, o nome, o endereço, o número de telefone, o número de fax e o endereço de correio electrónico.

A informação de contacto para este documento é a seguinte:

NOME	CONSELHO GESTOR DO SCEE
Morada:	Rua Professor Gomes Teixeira 350-265 Lisboa
Correio electrónico:	administrador@scee.gov.pt
Página Internet:	www.scee.gov.pt

---

Telefone	+ 351 213 927 600
Fax:	+351 213 927 997

---

Tabela 5 – Dados para contacto

---

### **1.5.3. ENTIDADE QUE DETERMINA A CONFORMIDADE DA DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO (DPC) PARA A POLÍTICA**

---

O Conselho Gestor do SCEE é o órgão competente para determinar a adequação das DPC das diversas entidades, com a Política de Certificados definida neste documento.

---

### **1.5.4. PROCEDIMENTOS PARA APROVAÇÃO DA DPC**

---

O Conselho Gestor do SCEE é a entidade responsável pela aprovação da presente PC e das PC e DPC associadas, bem como por garantir que as declarações de práticas de certificação das várias entidades certificadoras do Estado, bem como da entidade certificadora raiz do Estado, estão em conformidade com a política de certificação do SCEE.

---

### **1.6. DEFINIÇÕES E ACRÓNIMOS**

---

Ver Anexo D.

## 2. RESPONSABILIDADE DE PUBLICAÇÃO E REPOSITÓRIO

---

### 2.1. REPOSITÓRIOS

---

Um repositório é o conjunto de equipamentos (hardware e software), pessoas e procedimentos, construído com o objectivo de publicar, entre outras, informação relativa às práticas adoptadas e o estado dos certificados.

Neste ponto as entidades responsáveis pelas diversas DPC devem discriminar, no mínimo:

- a) Níveis de disponibilidade;
- b) os protocolos de acesso;
- c) mecanismos de segurança implementados.

### 2.2. PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICAÇÃO

---

Todos os repositórios no domínio da SCEE, deverão disponibilizar, no mínimo, a seguinte informação:

- a) Uma cópia electrónica deste documento (PCert), assinado electronicamente, por indivíduo devidamente autorizado e com certificado digital atribuído para o efeito;
- b) Uma cópia electrónica da sua DPC, assinada electronicamente, por indivíduo devidamente autorizado e com certificado digital atribuído para o efeito;
- c) Listas de Certificados Revogados (LCR)
- d) Lista de Certificados de Entidades Certificadoras Revogadas (LER), quando aplicável;
- e) Documentação de suporte (exemplo: formulários para pedido de certificado, pedido de revogação, etc.), num formato amplamente acessível;
- f) As LCR;
- g) Qualquer outra informação relevante deverá ser de igual modo publicada.

**As entidades integradas no domínio do SCEE deverão conservar todas as versões anteriores das suas PC (caso exista) e DPC, disponibilizando-as a quem o solicite (desde que justificado), ficando, no entanto fora do repositório público de acesso livre.**

**Os certificados para efeitos de confidencialidade serão os únicos certificados disponibilizados com acesso livre, no entanto, apenas e quando assim esteja estabelecido na respectiva DPC.**

Quando se trate dos repositórios das EC, e caso tenham sido criadas EC subordinadas ou ER, à informação referida anteriormente deve ser adicionada a mesma informação relacionada com as suas subordinadas.

Este documento pode ser consultado em: <http://www.scee.gov.pt/pcert>

### 2.3. PERIODICIDADE DE PUBLICAÇÃO

A informação incluída nos repositórios deverá ser disponibilizada logo que haja informação actualizada.

No que concerne às LCR, a sua publicação não deverá em caso algum exceder 24 horas desde a data da sua aprovação/criação até a sua publicação em repositório.

Independentemente, de haver ou não informação actualizada, devem ser considerados como prazos mínimos para actualização da informação os seguintes:

DOCUMENTO	PRAZOS	
Políticas de certificados da SCEE	Anualmente	
DPC		
Documentação de suporte		
Listas de certificados revogados	ECRaizEstado	2 meses
	ECEstado	1 mês
	subECEstado	1 semana

Tabela 6 – Prazos mínimos para renovação da informação pelas diversas entidades

### 2.4. CONTROLO DE ACESSO AOS REPOSITÓRIOS

No acesso à informação contida nos repositórios deverá ser garantido que esta apenas é disponibilizada, apenas e só, em modo de leitura.

Devem ser implementados mecanismos de segurança de forma a garantir que apenas pessoas autorizadas possam escrever ou modificar a informação contida nos repositórios.

A actual política não estabelece nenhum tipo de restrição de acesso para consulta das CRL, e ultimas versões das DPC e Política de Certificados.

### 3. IDENTIFICAÇÃO E AUTENTICAÇÃO

#### 3.1. ATRIBUIÇÃO DE NOMES

No domínio SCEE é permitida a atribuição e utilização de nomes Reais, Pseudónimos e equipamentos.

##### 3.1.1. TIPO DE NOMES

Todos os titulares de certificados requerem um nome único (DN - *Distinguished Name*) de acordo com o standard X.500.

Os certificados atribuídos a cada entidade deverão conter no campo "*Subject*", um DN, para utilização como identificador único de cada entidade, de acordo com o preconizado no RFC 3280, pelo que:

- a) Para os certificados emitidos a pessoas, o atributo descreve a organização a que o titular do certificado pertence;
- b) Nos certificados atribuídos a equipamentos, é inscrito o nome da organização responsável pela sua operação (patrocinador);
- c) O DN deverá ser sempre preenchido.

O campo "*Subject*" deverá ser construído seguindo o descrito na tabela seguinte, sendo obrigatória a utilização dos seguintes atributos:

ATRIBUTO	CÓDIGO	REGRAS PARA PREENCHIMENTO
CountryName	C	Incluir o código "PT".
OrganizationName	O	Este campo corresponde, regra geral, ao Ministério (ou equivalente) do titular do certificado.
OrganizationUnitName	OU	Neste campo deverá constar informação relativa ao organismo (ou equivalente) a que o titular do certificado pertence.
CommonName	CN	<p>É proibida a utilização de "<i>nicknames</i>".</p> <p>Os equipamentos deverão ser identificados através do modelo e número de série.</p> <p>Se os equipamentos forem servidores, estes serão designados pelo FODN (CN = "FODN".), sendo proibida a sua designação através do endereço IP.</p> <p>Nos certificados emitidos para pessoa colectiva, deverá ser incluído o nome da pessoa singular responsável pela sua utilização.</p> <p>Quando se trate de nomes reais, deverá corresponder</p>

		com o nome que aparece identificado no documento de Identificação.
		Quando se trate de pseudónimos, o nome deverá ser antecedido da expressão "Pseudo:".

Tabela 7 – Regras para o preenchimento do DN

### 3.1.2. NECESSIDADE DE NOMES SIGNIFICATIVOS

Os nomes utilizados dentro da cadeia de confiança do SCEE devem identificar de forma concreta e lógica a pessoa ou objecto a quem é atribuído um certificado digital.

As EC e ER, devem garantir que a relação entre o titular e a organização a que pertencem é a mesma que consta no certificado e é facilmente perceptível e identificável pelos Humanos.

### 3.1.3. ANONIMATO OU PSEUDÓNIMO DE TITULARES

Os titulares de certificados apenas podem optar pela utilização de pseudónimos. Neste caso o atributo "*CommonName*" do campo "*subject*" deverá começar pela identificação pela palavra "pseudo:", seguida do pseudónimo do titular (CN = pseudo: "qualquer cadeia de caracteres").

As entidades responsáveis pelo processo de registo podem recusar a aceitação de pseudónimos considerados ostensivos.

Não é permitida a utilização de titulares com base no conceito de anonimato.

### 3.1.4. INTERPRETAÇÃO DE FORMATO DE NOMES

As regras utilizadas pela SCEE para interpretar o formato dos nomes dos certificados que emite são as contidas na norma ISO 9595.

Seguir o estabelecido no RFC 3280, para certificados emitidos a partir de 31 de Dezembro de 2003, todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado, devem ser codificados numa *UTF8String*, com excepção dos atributos *country* e *serialnumber*, que devem estar codificados numa *PrintableString*.

### 3.1.5. UNICIDADE DE NOMES

Os identificadores do tipo DN deverão ser únicos para cada titular de certificado, dentro de cada EC e não podem induzir a ambiguidades.

Poderão ser utilizados caracteres adicionais ao nome original de cada entidade de forma a assegurar a unicidade do campo.

As DPC deverão descrever de forma clara os critérios que utilizam para garantir a unicidade dos nomes.

### **3.1.6. RECONHECIMENTO, AUTENTICAÇÃO E FUNÇÕES DAS MARCAS REGISTRADAS**

---

As entidades requisitantes de certificados, devem demonstrar que têm direito à utilização do nome requisitado.

Nas DPC devem estar explícitos os procedimentos utilizados para verificação do estipulado neste ponto.

### **3.2. VALIDAÇÃO DE IDENTIDADE NO REGISTO INICIAL**

---

Para os certificados emitidos no domínio da SCEE, é obrigatório que o registo inicial seja efectuado presencialmente, ou seja, a validação inicial da identidade do requerente é feita pelo método de “cara-a-cara”.

Nas DPC deve ser descrito todos os passos necessários, desde o início do pedido de certificado até à atribuição do certificado digital ao futuro titular.

#### **3.2.1. MÉTODO DE COMPROVAÇÃO DA POSSE DE CHAVE PRIVADA**

---

É considerado um mecanismo aceitável como método de comprovação da posse de chave privada a utilização do *Certificate Management Protocol* (CMP) definido no RFC 2510.

Pode ser permitida a utilização de outros métodos desde que o Conselho Gestor do SCEE verifique que o método proposto é no mínimo tão seguro como o descrito anteriormente.

Nas DPC deve estar descrito de forma clara o método utilizado para garantir a comprovação da posse de chave privada

#### **3.2.2. AUTENTICAÇÃO DA IDENTIDADE DE UMA PESSOA COLECTIVA**

---

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.

Assim, as EC (ou as ER) devem guardar toda a documentação utilizada para verificação da identidade, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, garantindo, no caso de o pedido ser subscrito para outrem, os poderes bastantes do requerente para a referida subscrição.

Entre outras, considera-se como documentação mínima exigível, a documentação onde conste todos os dados necessários para a criação e emissão do certificado digital.

Assim, quando requerido pela pessoa colectiva a constar como titular do certificado, é subscrito pelos seus representantes legais e contém, entre outros, os seguintes elementos:

- 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 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 quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- f) Eventual referência a uma qualidade específica, em função da utilização a que o certificado estiver destinado;
- g) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos.

Quando requerido por outrem que não o titular do certificado, o mesmo, para além dos elementos referidos no número anterior, contém, consoante seja requerido por pessoa singular ou colectiva, os seguintes elementos referentes ao requerente:

- a) Nome ou denominação legal;
- b) Número do bilhete de identidade, data e entidade emitente, ou qualquer outro elemento que permita a identificação inequívoca, ou número de pessoa colectiva;
- c) Residência ou sede;
- d) 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;
- e) Endereço e outras formas de contacto;
- f) Declaração da pessoa singular a constar como titular do certificado de que se obriga ao cumprimento das obrigações enquanto titular.

Nas DPC deve constar um exemplar do documento que serve de base ao registo do requerente.

---

### **3.2.3. AUTENTICAÇÃO DA IDENTIDADE DE UMA PESSOA SINGULAR**

---

O processo de autenticação da identidade de uma pessoa singular, deve obrigatoriamente garantir que a pessoa singular para quem vai ser emitido o certificado é quem na realidade diz ser:

Assim, as EC (ou as ER) devem guardar toda a documentação utilizada para verificação da identidade, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, garantindo, no caso de o pedido ser subscrito para outrem, os poderes bastantes do requerente para a referida subscrição.

Entre outras, considera-se como documentação mínima exigível, a documentação onde conste todos os dados necessários para a criação e emissão do certificado digital, destacando-se, os seguintes elementos:

- a) Nome completo;

- b) Indicação de eventual pseudónimo a constar como titular;
- c) Número do bilhete de identidade, data e entidade emitente ou qualquer outro elemento que permita a identificação inequívoca;
- d) Endereço e outras formas de contacto;
- e) Eventual indicação de uma qualidade específica em função da utilização a que este se destinar;
- f) Indicação quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- g) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos.

No caso de o pedido de emissão ser requerido por outrem que não a pessoa singular a constar como titular do certificado, o mesmo, para além dos elementos referidos no número anterior, contém, consoante seja requerido por pessoa singular ou colectiva, os seguintes elementos referentes ao requerente:

- a) Nome ou denominação legal;
- b) Número do bilhete de identidade, data e entidade emitente, ou qualquer outro elemento que permita a identificação inequívoca, ou número de pessoa colectiva;
- c) Residência ou sede;
- d) 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;
- e) Endereço e outras formas de contacto.
- f) Declaração da pessoa singular a constar como titular do certificado de que se obriga ao cumprimento das obrigações enquanto titular.

Nas DPC deve constar um exemplar do documento que serve de base ao registo do requerente.

---

### **3.2.4. INFORMAÇÃO DE SUBSCRITOR/TITULAR NÃO VERIFICADA**

---

Toda a informação descrita nos pontos 3.2.3 e 3.2.4, deve ser obrigatoriamente verificada.

As Entidades Certificadoras e as Entidades de Registo podem autorizar entidades privadas a tomar acções em nome de outras entidades, no entanto, tais autorizações estão geralmente associadas com regras particulares das instituições.

A autenticação das autorizações é uma parte formal do pedido de registo de certificado para entidades com personalidade jurídica.

Um certificado emitido é uma confirmação de que uma entidade legal é intitulada para utilizar uma chave privada em nome de outra entidade legal.

### 3.2.5. CRITÉRIOS PARA INTEROPERABILIDADE

---

Nos processos relativos a acordos de interoperabilidade, tendo por base certificação cruzada com Infra-estruturas de Chaves Públicas externas, será analisada, no mínimo, a seguinte documentação:

- a) A Política de Certificados;
- b) O ultimo 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;

O Conselho Gestor agirá em conformidade com o estabelecido no documento “SCEE - Regulamento para a interoperabilidade”, nos casos em que seja solicitado um pedido para acordo de interoperabilidade, com base em certificação cruzada.

### 3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE RENOVAÇÃO DE CHAVES

---

#### 3.3.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA RENOVAÇÃO DE CHAVES, DE ROTINA

---

A identificação e autenticação para a renovação de certificados pode realizar-se utilizando os procedimentos para a autenticação e identificação inicial, ou utilizando pedidos assinados digitalmente, mediante o certificado original que se pretende renovar, sempre que este tenha expirado e não exista pedido para a sua revogação.

#### 3.3.2. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA RENOVAÇÃO DE CHAVES, APÓS REVOGAÇÃO

---

A política de identificação e autenticação para a renovação de um certificado, depois deste ser revogado deve seguir as mesmas regras constantes no 3.2.2 e 3.2.3.

A renovação não deve ser concedida se:

- a) A revogação ocorreu porque o certificado foi emitido para uma pessoa que não a que está no *Subject* do certificado;
- b) O certificado foi emitido sem autorização da pessoa que está indicada no *Subject*;
- c) A entidade que aprovou o titular descobre que tem razões para acreditar que a informação dada para o certificado é falsa.

**As DPC devem descrever de forma clara as regras utilizadas.**

### 3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDO DE REVOGAÇÃO

---

As regras de identificação para os pedidos de revogação poderão ser as mesmas que para o registo inicial.

Qualquer entidade integrada no domínio da SCEE, 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.

**As DPC devem descrever de forma clara as regras utilizadas.**

---

## **4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO**

---

---

### **4.1. PEDIDO DE CERTIFICADO**

---

---

#### **4.1.1. QUEM PODE SUBSCREVER UM PEDIDO DE CERTIFICADO**

---

As DPC devem descrever de forma clara qual a comunidade que se aceita para subscrever um pedido de certificado.

---

#### **4.1.2. PROCESSO DE REGISTO E RESPONSABILIDADES**

---

O processo de registo para pedido de um certificado, deverá ser baseado pelo menos nas seguintes etapas:

- a) Estabelecimento do registo inicial do requisitante, tal como definido no ponto 3.2 “Validação de identidade no registo inicial”;
- b) Obtenção por parte do requisitante, do respectivo par de chaves, por cada certificado requisitado/solicitado;
- c) Assinatura por parte do requisitante de um documento onde esteja especificado os termos e condições aplicáveis à utilização do certificado.

As DPC devem descrever detalhadamente o processo de registo utilizado, nomeadamente, a documentação necessária, bem como a identificação das funções e responsabilidades dos diversos participantes no referido processo.

---

## **4.2. PROCESSAMENTO DO PEDIDO DE CERTIFICADO**

---

Os pedidos de certificado, depois de recebidos pela entidade competente (EC ou ER), são considerados válidos se os seguintes requisitos forem cumpridos:

- a) Recepção e verificação de toda a documentação e autorizações exigidas;
- b) verificação da identidade do requisitante;
- c) verificação da exactidão e integridade do pedido de certificado;
- d) criação e assinatura o certificado;
- e) disponibilização do certificado ao titular.

As DPC devem descrever detalhadamente todo o processo.

---

### **4.2.1. PROCESSOS PARA A IDENTIFICAÇÃO E FUNÇÕES DE AUTENTICAÇÃO**

---

De acordo com o estipulado na secção 3.2 deste documento.

A DPC deve indicar como e quem efectua as tarefas de identificação e autenticação, bem como os mecanismos que dispõe.

---

### **4.2.2. APROVAÇÃO OU RECUSA DE PEDIDOS DE CERTIFICADO**

---

A aprovação do certificado passa pelo cumprimento dos requisitos mínimos exigidos no ponto “4.2”. Quando tal não se verifique, a entidade competente (EC ou ER) pode recusar a emissão do certificado.

Estes procedimentos, aceitação ou recusa, serão processados de acordo com os requisitos estipulados na respectiva DPC da entidade.

As DPC devem descrever detalhadamente todo o processo.

---

### **4.2.3. PRAZO PARA PROCESSAR O PEDIDO DE CERTIFICADO**

---

Os pedidos de certificados serão processados sem atrasos, a partir do momento em que toda a documentação exigida, esteja na posse da entidade responsável pela emissão do certificado.

A DPC estabelece o prazo máximo necessário para o processamento dos pedidos de certificados.

---

## **4.3. EMISSÃO DE CERTIFICADO**

---

---

### **4.3.1. PROCEDIMENTOS PARA A EMISSÃO DE CERTIFICADO**

---

A emissão do certificado por parte de uma EC da SCEE, indica que todos os procedimentos até à emissão foram concluídos sucesso.

Os procedimentos estabelecidos nesta secção, são também aplicados aos casos de renovação de certificados, uma vez que implica a emissão de novos certificados.

Os procedimentos adoptados devem garantir que para a emissão de certificados a EC:

- a) Utiliza procedimentos de geração de certificados que vincula de forma segura, o certificado com a respectiva informação de registo (incluindo a chave pública certificada);
- b) depois de emitido o certificado, as notificações são efectuadas de acordo com estabelecido na secção 4.3.2 do presente capítulo;
- c) todos os certificados iniciam a sua vigência no momento da sua emissão, com excepção dos casos em que se indique nos próprios uma data e hora para a entrada em vigor diferente (que nunca poderá ser posterior ao dia natural da sua emissão);
- d) o período de validade do certificado está sujeito à extinção antecipada, temporal ou definitiva, quando se verificarem situações para a revogação ou suspensão.

As DPC devem descrever detalhadamente todo o processo, bem como a forma utilizada para entrega do certificado ao seu titular.

### 4.3.2. NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO AO TITULAR

---

No âmbito desta política, consideram-se como formas aceitáveis de notificação da emissão do certificado ao titular por parte da respectiva EC, as que se baseiam nas seguintes formas:

- a) Envio do certificado directamente à ER requisitante (quando aplicável);
- b) envio da informação necessária para que o titular possa descarregar o certificado de um sítio *Web* ou repositório;
- c) Envio da informação necessária para que a ER respectiva possa descarregar o certificado de um sítio *Web* ou repositório (quando aplicável);
- d) De forma presencial.

Em caso algum o futuro titular pode obter previamente o certificado sem o prévio procedimento de aceitação do mesmo.

Podem ser utilizadas outras formas de notificação para além das descritas anteriormente, desde que devidamente aprovadas pelo Conselho Gestor do SCEE e descritas na respectiva DPC.

A DPC deve descrever o método utilizado para a notificação da emissão do certificado ao titular.

### 4.4. ACEITAÇÃO DO CERTIFICADO

---

#### 4.4.1. PROCEDIMENTOS PARA A ACEITAÇÃO DE CERTIFICADO

---

Antes de ser disponibilizado o certificado ao titular, e conseqüentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, deverá ser garantido que:

- a) O titular toma conhecimento dos seus direitos e responsabilidades;
- b) o titular toma conhecimento das funcionalidades e conteúdo do certificado;
- c) o titular aceita formalmente sobre a aceitação do certificado e das suas condições de utilização assinando para o efeito, de forma manuscrita ou electronicamente, o Termo de Responsabilidade do Titular;

No termo de responsabilidade do titular, devem constar, pelo menos, os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo.

A DPC deve estabelecer os mecanismos para verificar a aceitação do certificado por parte de titular.

#### 4.4.2. PUBLICAÇÃO DO CERTIFICADO

---

As entidades certificadoras, na publicação/distribuição dos certificados, deve utilizar sistemas seguros que permitam a sua conservação e disponibilização para efeitos de verificação, assegurando que:

- a) Regra geral, a EC não publica o certificado do titular;
- b) o certificado é disponibilizado, integralmente, ao titular para quem foi emitido, com os constrangimentos definidos no ponto 4.4.1;
- c) O certificado só é publicamente disponibilizado com o consentimento do titular;

As DPC devem descrever detalhadamente todo o processo.

---

### **4.4.3. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO A OUTRAS ENTIDADES**

---

A Notificação da emissão de certificado pela EC respectiva é obrigatória apenas para o requisitante/titular do certificado. Se o pedido de certificado tiver como origem com recurso aos serviços de uma ER, esta entidade também deverá ser notificada.

---

### **4.5. USO DO CERTIFICADO E PAR DE CHAVES**

---

Dentro da comunidade da SCEE, a utilização dos certificados e respectiva chave privada, pelos diversos participantes, segue os seguintes constrangimentos:

- a) A ECRaizEstado apenas emite certificados à ECEstado e EC externas e ao pessoal próprio para efeitos de operação dos seus sistemas;
- b) As ECEstado emitem certificados ao pessoal próprio para efeitos de operação dos seus sistemas e dependendo da forma como estão organizadas, emitem certificados para o utilizador final (titulares) ou para subECEstado;

As EC devem assegurar que a utilização da sua chave privada apenas é utilizada para assinar certificados e CRL. É ainda responsabilidade das EC, garantir que as chaves privadas atribuídas ao seu pessoal para efeitos de operação do sistema, são utilizadas apenas e exclusivamente para esse fim.

---

#### **4.5.1. USO DO CERTIFICADO E DA CHAVE PRIVADA PELO TITULAR**

---

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

A sua utilização apenas é permitida:

- a) a quem estiver designado no campo “*Subject*” do certificado;
- b) depois de aceitar as condições definidas nos pontos 1.4.1 e 1.4.2; e
- c) enquanto este se mantiver válido.

As DPC devem descrever o tipo de certificados emitidos e sua utilização, podendo estabelecer limitações adicionais.

---

### **4.5.2. 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 apenas o que é estabelecido nesta política e na respectiva 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 Políticas e práticas de certificação;
- d) verificar os certificados (validação de cadeias de confiança) e CRL, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
- e) confiar nos certificados, utilizando-os sempre que estes estejam válidos;

---

### **4.6. RENOVAÇÃO DE CERTIFICADOS**

---

A renovação de um certificado é o processo em que a emissão de um novo certificado, no qual é inscrito uma nova validade. Este processo utiliza os dados anteriores do certificado, não havendo alteração das chaves ou qualquer outra informação, com excepção do período de validade do certificado.

Este processo levanta algumas reticências uma vez que a sua utilização é caracterizada pela perda de entropia das chaves, uma vez que não são gerados novos parâmetros, mas sim utilizados os já existentes.

Esta prática não é suportada na SCEE.

---

#### **4.6.1. MOTIVOS PARA RENOVAÇÃO DE CERTIFICADO**

---

Não aplicável.

---

#### **4.6.2. QUEM PODE SUBMETTER O PEDIDO DE RENOVAÇÃO DE CERTIFICADO**

---

Não aplicável.

---

#### **4.6.3. PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DE CERTIFICADO**

---

Não aplicável.

---

#### **4.6.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO AO TITULAR**

---

Não aplicável.

---

### **4.6.5. PROCEDIMENTOS PARA ACEITAÇÃO DE CERTIFICADO**

---

Não aplicável.

---

### **4.6.6. PUBLICAÇÃO DE CERTIFICADO APÓS RENOVAÇÃO**

---

Não aplicável.

---

### **4.6.7. NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO A OUTRAS ENTIDADES**

---

Não aplicável.

---

## **4.7. RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES**

---

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

A emissão do certificado é feita de acordo com o estabelecido na secção 4.3.

---

### **4.7.1. MOTIVOS PARA A RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES**

---

De forma geral, são considerados motivos válidos para a renovação de certificado com geração de novo par de chaves, sempre e quando que se verifique que:

- a) O certificado esteja a expirar;
- b) o suporte do certificado esteja expirar;
- c) a informação do certificado sofra alterações.

As DPC devem descrever quais os motivos para a renovação de certificado com geração de novo par de chaves.

---

### **4.7.2. QUEM PODE SUBMETER O PEDIDO DE CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA**

---

A submissão do pedido de certificação, é válida para titulares com certificados em vigor.

---

### **4.7.3. PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES**

---

As DPC devem descrever os processos para os pedidos de renovação, identificando os diferentes cenários e os respectivos requisitos.

---

### **4.7.4. NOTIFICAÇÃO DA EMISSÃO DE NOVO CERTIFICADO AO TITULAR**

---

De acordo com os critérios especificados para a emissão inicial de certificados.

---

### **4.7.5. PROCEDIMENTOS PARA ACEITAÇÃO DE UM CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES**

---

A recepção do certificado renovado, por si só, serve como confirmação da aceitação do mesmo.

As DPC devem descrever de forma clara os procedimentos adoptados, no entanto, podem ser estabelecidos requisitos mais restritivos.

---

### **4.7.6. PUBLICAÇÃO DE NOVO CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES**

---

De acordo com os critérios especificados para a emissão inicial de certificados.

---

### **4.7.7. NOTIFICAÇÃO DA EMISSÃO DE NOVO CERTIFICADO A OUTRAS ENTIDADES**

---

De acordo com os critérios especificados para a emissão inicial de certificados.

---

## **4.8. MODIFICAÇÃO DE CERTIFICADOS**

---

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

Esta prática é suportada pela SCEE com restrições, nomeadamente, na informação sujeita a alterações não está contemplada a alteração da validade inicial do certificado.

Os procedimentos descritos nos seguintes parágrafos, relativos à alteração de certificados, estão sujeitas às mesmas regras definidas para os pedidos de certificado em conformidade com o disposto no ponto 4.1.

---

### **4.8.1. MOTIVOS PARA ALTERAÇÃO DE CERTIFICADO**

---

Descrito na secção “4.8”.

---

### **4.8.2. QUEM PODE SUBMETER O PEDIDO DE ALTERAÇÃO DE CERTIFICADO**

---

Descrito na secção “4.8”.

---

### **4.8.3. PROCESSAMENTO DO PEDIDO DE ALTERAÇÃO DE CERTIFICADO**

---

Descrito na secção “4.8”.

---

### **4.8.4. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO ALTERADO AO TITULAR**

---

Descrito na secção “4.8”.

---

### **4.8.5. PROCEDIMENTOS PARA ACEITAÇÃO DE CERTIFICADO ALTERADO**

---

Descrito na secção “4.8”.

---

### **4.8.6. PUBLICAÇÃO DO CERTIFICADO ALTERADO**

---

Descrito na secção “4.8”.

---

### **4.8.7. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO ALTERADO A OUTRAS ENTIDADES**

---

Descrito na secção “4.8”.

---

## **4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO**

---

A revogação e suspensão de certificados, são mecanismos a utilizar quando por algum motivo os certificados deixam de ser fiáveis, antes do período de finalização originalmente previsto.

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

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

---

### **4.9.1. MOTIVOS PARA A REVOGAÇÃO**

---

Os certificados devem ser revogados, sempre que se verifiquem as seguintes situações:

- a) Roubo, extravio, destruição ou deterioração do dispositivo de suporte dos certificados (exemplo: *Smartcard*);
- b) Incapacidade ou falecimento do titular;
- c) Inexactidões graves nos dados fornecidos;
- d) o certificado estar suspenso por um período alargado;
- e) comprometimento ou suspeita de comprometimento das chaves privada do titular;
- f) comprometimento ou suspeita de comprometimento da senha (exemplo: PIN);
- g) comprometimento ou suspeita de comprometimento das chaves privada da EC;
- h) incumprimento por parte da EC ou titular das responsabilidades prevista na DPC;

- i) sempre que haja razões credíveis que induzam que o serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- j) por resolução judicial ou administrativa;
- k) por vontade do próprio.

As DPC devem estabelecer de forma detalhada as causas passíveis para revogação do certificado.

---

### 4.9.2. QUEM PODE SUBMETER O PEDIDO DE REVOGAÇÃO

---

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 4.9.1, os seguintes:

- a) O titular do certificado;
- b) O responsável por um certificado emitido para produtos de tecnologia de informação;
- c) uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos;
- d) a EC ou ER;
- e) a Entidade de Certificação Electrónica do Estado;
- f) o Conselho Gestor do SCEE;
- g) a Autoridade Credenciadora.

**As DPC devem descrever as entidades a quem é permitido submeter o pedido de revogação.**

---

### 4.9.3. PROCEDIMENTO PARA O PEDIDO DE REVOGAÇÃO

---

De modo geral os procedimentos mínimos a ter em conta para um pedido de revogação serão os seguintes:

- a) Qualquer pedido de revogação deve ser sempre autenticado e autorizado;
- b) Todos os pedidos de revogação devem ser endereçados para a EC ou ER respectiva;
- c) Os pedidos podem ser efectuados por escrito ou por um processo on-line (CMP);
- d) Qualquer pedido, desde que autenticado, deve ficar registado e arquivado;
- e) Sempre que um certificado for revogado, deve ficar documentado juntamente com uma descrição exaustiva do motivo da revogação, nomeadamente:
  - i. data do pedido de revogação;
  - ii. nome do titular do certificado (o assinante);
  - iii. exposição pormenorizada dos motivos para o pedido de revogação;
  - iv. nome e funções da pessoa que solicita a revogação;

- v. informação de contacto da pessoa que solicita a revogação;
  - vi. assinatura da pessoa que solicita a revogação.
- f) sempre que for revogado um certificado de um titular, a revogação deve ser publicada na respectiva LCR.

As DPC devem estabelecer de forma detalhada os procedimentos utilizados para o pedido de revogação de certificados.

---

#### **4.9.4. 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.

---

#### **4.9.5. 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.

---

#### **4.9.6. REQUISITOS DE VERIFICAÇÃO DA REVOGAÇÃO PELAS PARTE CONFIANTES**

---

Antes de utilizarem um certificado, as partes confiantes tem como responsabilidade verificar o estado de todo os certificados, através das LCR ou num servidor de verificação do estado on-line (via OCSP).

---

#### **4.9.7. PERIODICIDADE DA EMISSÃO DA LISTA DE CERTIFICADOS REVOGADOS (LCR)**

---

As EC deverão publicar 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 se tiver produzido as várias entidades deverão disponibilizar nova informação de revogação com os seguintes limites máximos:

- a) para as EC que emitam certificados de utilizador final, as LCR serão disponibilizadas a cada 24 Horas;
- b) para as EC que não emitam certificados de utilizador final, as LCR serão disponibilizadas a cada 3 meses;

As DPC devem estabelecer de forma detalhada a periodicidade utilizada para emissão das LCR.

---

#### **4.9.8. PERÍODO MÁXIMO ENTRE A EMISSÃO E A PUBLICAÇÃO DA CRL**

---

De acordo com o ponto 4.9.7

---

### **4.9.9. DISPONIBILIDADE DE VERIFICAÇÃO ON-LINE DO ESTADO / REVOGAÇÃO DE CERTIFICADO**

---

As DPC deverão estabelecer se dispõem e em que condições, serviços de validação do estado dos certificados de forma on-line.

---

### **4.9.10. REQUISITOS DE VERIFICAÇÃO ON-LINE DE REVOGAÇÃO**

---

No caso de serem utilizadas as AV, as partes confiantes deverão dispor de *software* capaz de operar o protocolo OCSP, de forma a obter a informação sobre o estado do certificado.

---

### **4.9.11. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO**

---

Não estabelecido.

---

### **4.9.12. REQUISITOS ESPECIAIS EM CASO DE COMPROMETIMENTO DE CHAVE PRIVADA**

---

Apenas quando se trate do comprometimento da chave privada de uma EC. Neste caso deverão ser adoptados os procedimentos descritos na secção 5.7.3.

---

### **4.9.13. MOTIVOS PARA SUSPENSÃO**

---

As DPC deverão os motivos e identificar as causas em que se aplica a suspensão do certificado em detrimento da revogação.

---

### **4.9.14. QUEM PODE SUBMETER O PEDIDO DE SUSPENSÃO**

---

A estabelecer na DPC.

---

### **4.9.15. PROCEDIMENTOS PARA PEDIDO DE SUSPENSÃO**

---

A estabelecer na DPC.

---

### **4.9.16. LIMITE DO PERÍODO DE SUSPENSÃO**

---

A estabelecer na DPC.

---

## **4.10. SERVIÇOS SOBRE O ESTADO DO CERTIFICADO**

---

---

### **4.10.1. CARACTERÍSTICAS OPERACIONAIS**

---

Caso haja algum serviço para além das LCR, será um serviço de validação on-line, com implementação do protocolo OCSP, de acordo com o estipulado no RFC 2560.

---

### **4.10.2. DISPONIBILIDADE DE SERVIÇO**

---

Salvo causa justificada, a disponibilidade do serviço será contínua (24 horas, todos os dias do ano).

---

### **4.10.3. CARACTERÍSTICAS OPCIONAIS**

---

Para usufruir do serviço de validação on-line, as partes confiantes deverão dispor de um cliente OCSP que cumpra o RFC 2560.

---

### **4.11. FIM DE SUBSCRIÇÃO**

---

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

- a) Revogação do certificado;
- b) por ter caducado o prazo de validade do certificado.

---

### **4.12. RETENÇÃO E RECUPERAÇÃO DE CHAVES (*KEY ESCROW*)**

---

---

#### **4.12.1. POLÍTICAS E PRÁTICAS DE RECUPERAÇÃO DE CHAVES**

---

Apenas é autorizada a retenção de chaves para os seguintes casos:

- a) Chaves privadas das EC;
- b) Chaves para efeitos de confidencialidade.

Em ambos os casos apenas é permitido a realização desta operação, no mínimo por duas pessoas. As políticas e práticas de recuperação fazem parte integral da DPC da entidade.

---

#### **4.12.2. POLÍTICAS E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVES DE SESSÃO.**

---

Não estipulado.

---

## 5. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

---

---

### 5.1. MEDIDAS DE SEGURANÇA FÍSICA

---

Todos os aspectos relacionados com as medidas de segurança física exigidas às instalações onde operam as EC da SCEE, estão definidos no documento “Localização e Instalação das EC do SCEE – Medidas de Segurança Física”. Nesta secção apenas são descritos os aspectos mais relevantes.

---

#### 5.1.1. LOCALIZAÇÃO FÍSICA E TIPO DE CONSTRUÇÃO

---

As instalações das EC devem ser desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, devendo estar fisicamente protegidas do acesso não autorizado, dano, ou interferência. Esta protecção deve ser proporcional aos riscos identificados.

A arquitectura deverá ser formada aplicando o conceito de defesa em profundidade, ou seja, por níveis de segurança. 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).

Neste contexto torna-se fundamental a existência e integração de um conjunto de subsistemas, que em conjunto formam um sistema complementar de segurança electrónico, de funcionamento ininterrupto, proporcionando um ambiente altamente seguro.

O local onde se desenvolve a actividade da EC, a Zona de Alta Segurança (ZAS), é uma área deverá obedecer ao descrito para as áreas de Classe 1<sup>2</sup>. Esta área deverá ter as 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 em aço, com as dobradiças fixas e ombreira igualmente em aço, com de fechadura de segurança accionável electronicamente, características corta – fogo e funcionalidade anti-pânico.

---

#### 5.1.2. ACESSO FÍSICO AO LOCAL

---

O acesso à ZÁS, deverá ser composto por diversos perímetros com diferentes requisitos de segurança e autorizações. Entre os equipamentos que protegem os perímetros de segurança deverão incluir-se sistemas electrónicos de controlo de acessos, sistemas de vídeo vigilância e de gravação em circuito fechado de TV e sistemas de detecção de intrusões. Os vários sistemas devem estar integrados, funcionando de forma ininterrupta 24 horas, todos os dias do ano.

As ZÁS não podem ser contíguas às zonas de acesso comum do edifício. O acesso às mesmas, para actividades como emissão de certificados, deverá ser registado e gravado automaticamente sendo que o acesso deve ser feito através de pelo menos a conjugação

---

<sup>2</sup> Resolução do Conselho de Ministros n.º 50/88.

de dois sistemas, em que um deles é obrigatoriamente com recurso a tecnologia baseada em biometria.

Nas ZÁS, deve existir um livro para registo manual dos acessos e de todas as actividades e cerimónias que ocorram no seu interior.

---

### **5.1.3. ENERGIA E AR CONDICIONADO**

---

As instalações devem dispor de sistemas de alimentação 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 sistema de acondicionamento ambiental deverá ser composto por vários equipamentos independentes com capacidade para manter níveis de temperatura e humidade de acordo com recomendações para operação dos sistemas.

---

### **5.1.4. EXPOSIÇÃO À ÁGUA**

---

As ZAS devem dispor de detectores de inundação e sistemas de alarme apropriados para o efeito.

---

### **5.1.5. PREVENÇÃO E PROTECÇÃO CONTRA INCÊNDIO**

---

Os funcionários e os equipamentos devem ter todas as condições de segurança no que se concerne a incêndios.

As ZAS devem dispor de sistemas automáticos de detecção e extinção de incêndios.

Os materiais da sala e portas utilizadas devem ser de material não combustível e que sejam resistentes ao fogo, sendo que no caso das portas estas devem ter uma resistência de pelo menos 2 horas.

---

### **5.1.6. SALVAGUARDA DE SUPORTES DE ARMAZENAMENTO**

---

Os suportes de informação sensível, deverão ser armazenados de forma segura em cofres de acordo com o tipo de suporte e classificação da informação. O acesso a estas zonas, deve ser restrito a pessoas devidamente autorizadas.

---

### **5.1.7. ELIMINAÇÃO DE RESÍDUOS**

---

A eliminação de suportes magnéticos, ópticos e informação em papel, deve ser realizada de forma segura, seguindo os procedimentos estabelecidos para este fim, recorrendo a processos de desmagnetização, de esterilização e de destruição ou triturando em função do tipo de suporte a tratar. Periféricos criptográficos devem ser destruídos de acordo com as recomendações dos respectivos fabricantes.

### **5.1.8. INSTALAÇÕES EXTERNAS (ALTERNATIVA) PARA RECUPERAÇÃO DE SEGURANÇA**

---

Todas as cópias de segurança (e.g., base de dados, programas, file system,) devem ser colocadas em site remoto que será geograficamente separado do sítio primário.

As condições de segurança do site remoto deverão ser idênticas ou superiores ao estipulado para o local primário. O acesso é restrito apenas ao pessoal autorizado.

### **5.2. MEDIDAS DE SEGURANÇA DOS PROCESSOS**

---

Os sistemas de informação e os serviços disponibilizados pelas várias EC que integram a SCEE, devem ser operados de forma controlada.

#### **5.2.1. FUNÇÕES DE CONFIANÇA**

---

As funções de confiança a estabelecer deverão estar em conformidade com os requisitos estabelecidos no ponto “5.1.1” do documento CWA 14167 – parte 1, de Junho de 2003, para certificados qualificados.

Nas funções de confiança está incluído todo o pessoal com acesso aos sistemas de certificação das EC e que na prática podem materialmente afectar:

- a) Manipulação de informações de subscritor e validação de informação de emissão de Certificado;
- b) Funções do ciclo de vida dos certificados;
- c) Configuração e manutenção dos sistemas de certificação.

No âmbito da sua estrutura organizativa são consideradas funções de confiança as descritas a seguir, estando divididas e diferenciadas pela natureza da sua actividade, quer se trate das *software* para certificação digital, quer se trate das funções relacionadas com o dispositivo seguro para criação de assinaturas. A cada uma delas são cometidas as seguintes responsabilidades consoante o âmbito.

##### **5.2.1.1. Software para certificação digital**

---

- a) Administrador de Segurança (AdmSeg), responsáveis segurança global dos sistemas, nomeadamente, pela gestão e implementação das regras e práticas de segurança;
- b) Administrador de registo (AdmReg), responsáveis pela aprovação da emissão, suspensão e revogação de certificados de titulares;
- c) Administrador de Sistemas (AdmSist), responsáveis pela instalação, configuração e manutenção dos sistemas, no entanto, com acesso controlado às configurações relacionadas com a segurança;
- d) Operador de Sistemas (OpSist), responsáveis pela operação de rotina dos sistemas, estando autorizados a realizar as cópias de segurança e sua recuperação;
- e) Auditor de Sistemas (AuditorS), responsáveis pela análise da actividade do sistema, estão autorizados a ver e monitorizar os arquivos de actividade dos sistemas.

As DPC devem descrever em detalhe as responsabilidades inerentes a cada função.

### **5.2.1.2. Dispositivo seguro para criação de assinaturas**

---

- a) Administradores do HSM (AdmHSM), responsáveis pela segurança das chaves;
- b) Operadores do HSM (OpHSM), autorizados a utilizarem a chaves.

As DPC devem descrever em detalhe as responsabilidades inerentes a cada função.

### **5.2.2. NÚMERO DE PESSOAS EXIGIDAS POR TAREFA**

---

As seguintes tarefas/acções/actividade, requerem o mínimo a presença 2 pessoas em simultâneo:

- a) Qualquer acesso à ZÁS;
- b) Geração das chaves da EC;
- c) configuração dos perfis para o desempenho das funções de confiança
- d) manutenção e actualização dos sistemas dos sistemas;
- e) recuperação de chaves para efeitos de confidencialidade; e
- f) recuperação das chaves da EC.

As DPC devem descrever em detalhe a metodologia e o número de pessoas por tarefa adoptada.

### **5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA FUNÇÃO**

---

Todos os utilizadores autorizados, devem identificar-se preferencialmente através de certificados digitais emitidos pela própria EC.

No caso dos HSM são empregues as técnicas de segredo partilhado.

As DPC devem descrever em detalhe os mecanismos adoptados.

### 5.2.4. FUNÇÕES QUE REQUEREM SEPARAÇÃO DE RESPONSABILIDADES

De acordo com o descrito no quadro seguinte:

	AdmSeg	AdmReg	AdmSist	OpSist	AuditorS	AdmHSM *	opHSM *
AdmSeg			×		×		
AdmReg					×		
AdmSist	×				×		
OpSist							
AuditorS	×	×	×			×	×
AdmHSM *					×		
OpHSM. *					×		

#### NOTAS

× - As funções assinaladas são incompatíveis;

\*- Estas funções não são obrigatoriamente requeridas pela legislação, nem necessárias a todas as entidades certificadoras, podendo no entanto ser necessárias em casos específicos.

Tabela 8 – Incompatibilidade entre funções

### 5.3. MEDIDAS DE SEGURANÇA DE PESSOAL

As DPC devem descrever em detalhe os requisitos adoptados nas diversas secções, no entanto, a EC deve garantir que o pessoal com funções de confiança cumpre os seguintes requisitos mínimos:

- Nomeado formalmente para a função;
- ter recebido formação e treino adequado para o desempenho da respectiva função;
- garantir que o funcionário (p.e: contrato, estatuto próprio, etc.), não revela informação sensível sobre a EC ou dados de identificação dos titulares;
- garantir que o funcionário, (p.e: contrato, estatuto próprio, etc.), conhece os termos e condições para o desempenho da respectiva função; e
- garantir que o funcionário não desempenha funções que possam causar conflito com as suas responsabilidades nas actividades da EC

### 5.3.1. REQUISITOS RELATIVOS ÀS QUALIFICAÇÕES, EXPERIÊNCIA, ANTECEDENTES E CREDENCIAÇÃO

O pessoal que desempenha funções nas EC deve possuir suficientes qualificações para o desempenho da função.

### 5.3.2. PROCEDIMENTOS 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 credenciação varia tendo em conta a função de confiança e o tipo de EC onde se desenvolvem as actividades.

O grau de credenciação de segurança<sup>3</sup> exigido está descrito no quadro seguinte:

	ECRAIZESTADO	ECESTADO	SUBCESTADO	ERESTADO
AdmSeg	Secreto	Confidencial	Confidencial	Confidencial
AdmReg	Secreto	Confidencial	Confidencial	Confidencial
AdmSist	Secreto	Confidencial	Confidencial	Confidencial
OpSist	Secreto	Confidencial	Confidencial	Confidencial
AuditorS	Secreto	Confidencial	Confidencial	Confidencial
AdmHSM	Secreto	Confidencial	Confidencial	Confidencial
OpHSM.	Secreto	Confidencial	Confidencial	Confidencial

Tabela 9 – Credenciação de segurança

### 5.3.3. REQUISITOS DE FORMAÇÃO E TREINO

Os elementos com cargos que desempenhem actividades nas várias EC, deverão estar sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

- Certificação digital e Infra-estruturas de Chave Publica;
- Conceitos gerais sobre segurança da informação
- Formação específica para o seu posto
- Funcionamento do software e/ou hardware usado pela EC
- Política de Certificados e Declaração de Práticas de Certificação;
- Recuperação face a desastres;
- Procedimentos para a continuidade da actividade;
- Aspectos legais básicos relativos à prestação de serviços de certificação.

<sup>3</sup> Resolução do Conselho de Ministros n.º 50/88 (SEGNAC I), Capítulo 4

---

### **5.3.4. FREQUÊNCIA E REQUISITOS PARA ACÇÕES DE RECICLAGEM**

---

Sempre que existe qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, dever levar-se a cabo a adequada formação para todo o pessoal afecto às EC.

Sempre que sejam levadas a cabo alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação devem ser realizadas sessões formativas aos elementos das EC.

---

### **5.3.5. FREQUÊNCIA E SEQUÊNCIA DA ROTAÇÃO DE FUNÇÕES**

---

Não é definido nenhum plano de rotação na atribuição de tarefas ao pessoal das EC, contudo sempre que alguma EC o faça deve materializar de forma clara a forma como esta rotação é realizada

---

### **5.3.6. SANÇÕES PARA ACÇÕES NÃO AUTORIZADAS**

---

No caso da realização de acções não autorizadas respeitantes às EC, devem ser tomadas as medidas disciplinares adequadas.

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

Se for realizada alguma infracção, a EC suspenderá o acesso a todos os sistemas de EC de forma imediata às pessoas envolvidas com o conhecimento destes

Adicionalmente em função da gravidade da infracção cometida, devem aplicar-se as sanções previstas na lei geral da função pública, das organizações ou entidades.

---

### **5.3.7. CONTRATAÇÃO DE PESSOAL**

---

O pessoal contratado para exercer cargos relacionados com funções de confiança de qualquer parte da EC ou ER está sujeito aos mesmos critérios que um funcionário dos quadros da própria organização e é credenciado de acordo com o especificado na secção "5.3.2".

---

### **5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL**

---

Ao pessoal com cargos nas várias EC deve ser disponibilizado, no mínimo, os seguintes documentos:

- a) Política de Certificados
- b) Declaração de Práticas de Certificação
- c) Documento com a descrição das responsabilidades, obrigações e tarefas para a respectiva função;
- d) Documentação técnica sobre o software e hardware da EC.

---

### 5.4. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

---

---

#### 5.4.1. TIPO DE EVENTOS REGISTRADOS

---

As EC devem registar entre outros, os eventos especificado no documento CWA 14167-1, sendo obrigatório o registo dos seguintes:

- a) Ligar e desligar os servidores;
- b) Tentativas com sucesso ou fracassadas de alteração dos parâmetros de segurança do sistema operativo;
- c) Tentativas com sucesso ou fracassadas de criar, modificar, apagar contas do sistema
- d) Ligar e desligar as aplicações e sistemas utilizados para a actividade de certificação;
- e) Tentativas com sucesso ou fracassadas de início e fim de sessão;
- f) Tentativas com sucesso ou fracassadas das operações relativas ao pedido, emissão, renovação, modificação e revogação chaves e certificados;
- g) Tentativas com sucesso ou fracassadas de gerar ou emitir LCR;
- h) Tentativas com sucesso ou fracassadas de criar, modificarmos ou apagar informação dos titulares dos certificados;
- i) Tentativas com sucesso ou fracassadas de acesso às ZÁS da EC;
- j) Copias de segurança, recuperação ou arquivo dos dados;
- k) Alterações ou actualizações de software e hardware;
- l) Manutenção do sistema;
- m) Mudança de pessoal;

O registo dos eventos, efectuado com recurso a meios automáticos e/ou manuais, devem conter, pelo menos, a data e hora do evento, bem como a identificação da entidade causadora do evento.

Os eventos registados devem ser especificados na respectiva DPC.

---

#### 5.4.2. FREQUÊNCIA DA AUDITORIA DE REGISTOS

---

A auditoria dos registos deve ser realizadas com uma frequência mínima semanal e todos os eventos significativos devem ficar registados num relatório sumário de análise de eventos. Cada EC deve declarar na sua DPC a frequência com que auditoria de registos é implementada e quais os tipos de eventos considerados como significativos e que justificam a sua inclusão no Relatório Sumário de Análise de Eventos (RSAE).

---

#### 5.4.3. PERÍODO DE RETENÇÃO DOS REGISTOS DE AUDITORIA

---

As EC deverão guardar os registos de auditoria nos sistemas por um período mínimo de 3 meses. Depois de arquivados, os registos de auditoria devem ser conservados por um período mínimo de 20 anos.

Nas DPC deve ser especificado quais os períodos adoptados para a retenção dos registos de auditoria.

---

### **5.4.4. PROTECÇÃO DOS REGISTOS DE AUDITORIA**

---

Os registos de auditoria devem estar protegidos contra acessos não autorizados, alteração e destruição.

Por regra, os registos electrónicos devem estar protegidos com recurso a técnicas criptográficas, para que ninguém, com excepção das próprias aplicações de visualização de registos, com o controlo de acessos adequado, possam aceder aos mesmos.

Os registos manuais devem ser armazenados em local, que cumpra os requisitos definidos anteriormente, dentro das instalações seguras das EC.

A destruição de um arquivo de auditoria só pode ser levado a cabo com a autorização do Administrador de Sistema, Administrador de Segurança e Auditor de Registo. Esta destruição só pode proceder-se por recomendação escrita de qualquer dos três elementos.

Os registos de auditoria são considerados informação sensível como especificado na secção “9.4”.

---

### **5.4.5. PROCEDIMENTOS PARA A CÓPIA DE SEGURANÇA DOS REGISTOS**

---

Devem ser realizadas cópias de segurança dos registos de auditoria bem como dos RSAE.

As DPC devem descrever a os mecanismos adoptados para efectuar as cópias de segurança dos registos e RSAE.

---

### **5.4.6. SISTEMA DE RECOLHA DE DADOS DE AUDITORIA (INTERNO/EXTERNO)**

---

O sistema de recolha dos dados de auditoria deve ser uma combinação de processos automáticos e manuais executados pelos sistemas operativos, pelas aplicações das EC e pelo pessoal que as opera.

As DPC devem descrever de forma clara o procedimento para este sistema.

---

### **5.4.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS**

---

Não esta contemplada qualquer notificação. As DPC, caso implementem notificações, devem descrever o método e as pessoas/sistemas alvo de notificação.

---

### **5.4.8. AVALIAÇÃO DE VULNERABILIDADES**

---

Não havendo alterações significativas no ambiente global da EC, deve ser efectuada pelo menos uma vez por ano uma avaliação das vulnerabilidades.

O resultado da análise deve ser reportado ao responsável da EC para rever e aprovar, caso se justifique, um plano de implementação e correcção das vulnerabilidades detectadas.

---

### 5.5. ARQUIVO DE REGISTOS

---

---

#### 5.5.1. TIPO DE DADOS ARQUIVADOS

---

As EC devem arquivar, pelo menos os seguintes tipos de dados:

- a) Os registos de auditoria especificados no ponto 5.4 deste documento;
- b) As cópias de segurança dos sistemas que compõem a infra-estrutura da EC;
- c) Documentação relativa ao ciclo de vida dos certificados.
- d) Chaves para efeitos de confidencialidade (quando aplicável);
- e) Contratos estabelecidos entre a EC e outras entidades.

Nas DPC deve estar especificados o tipo de dados sujeitos a arquivos.

---

#### 5.5.2. PERÍODO DE RETENÇÃO EM ARQUIVO

---

Os dados sujeitos a arquivo são retidos por um período mínimo de 20 anos.

---

#### 5.5.3. PROTECÇÃO DOS ARQUIVOS

---

De acordo com o disposto na secção “5.4.4”.

---

#### 5.5.4. PROCEDIMENTOS PARA AS CÓPIAS DE SEGURANÇA DO ARQUIVO

---

De acordo com o disposto na secção “5.4.5”.

---

#### 5.5.5. REQUISITOS PARA VALIDAÇÃO CRONOLÓGICA DOS REGISTOS

---

Os registos arquivados são certificados por assinatura electrónica qualificada com validação cronológica que liga criptograficamente os dados com os valores de tempo.

Assim, os sistemas de informação utilizados pelas EC devem garantir o registo da data e hora do momento, tendo por base uma fonte de tempo segura.

Os sistemas da EC devem estar sincronizados entre si e as fontes de tempo utilizadas, devem-se calibrar automaticamente, devendo ser utilizada com referência a fonte de tempo do Observatório Astronómico de Lisboa (<http://www.oal.ul.pt>).

---

#### 5.5.6. SISTEMA DE RECOLHA DE DADOS DE ARQUIVO (INTERNO/EXTERNO)

---

De acordo com o disposto na secção “5.4.6”.

---

### **5.5.7. PROCEDIMENTOS DE RECUPERAÇÃO E VERIFICAÇÃO DE INFORMAÇÃO ARQUIVADA**

---

Só o pessoal devidamente autorizado deve ter acesso aos arquivos.

As EC devem verificar a integridade da informação arquivada a cada 9 meses, de forma a garantir que os mesmos se encontram em bom estado e que podem ser recuperados.

As EC devem garantir a capacidade para realizar verificações de integridade dos arquivos electrónicos na altura da sua criação. No caso de erros ou comportamentos imprevistos, deve ser criado um evento de segurança e ser criado novo arquivo.

As DPC devem descrever de forma clara os mecanismos utilizados.

---

### **5.6. RENOVAÇÃO DE CHAVES**

---

Apenas os titulares de certificados válidos podem requerer a renovação do respectivo par de chaves.

As DPC devem descrever de forma clara os processos utilizados para a renovação de certificado com geração de novo par de chaves (*re-key*), bem como os prazos mínimos exigidos para iniciar o processo de renovação.

---

### **5.7. RECUPERAÇÃO EM CASO DE DESASTRE OU COMPROMETIMENTO**

---

As DPC de cada EC deverão indicar, no caso de indisponibilidade das instalações da Entidade Certificadora qual o tempo máximo para esta indisponibilidade antes de ser activado o Plano de Continuidade de Serviço da respectiva EC.

O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade de disponibilidade estão disponíveis no Local Alternativo, devendo a DPC indicar o tempo máximo para activação dos serviços.

---

#### **5.7.1. PROCEDIMENTOS EM CASO DE INCIDENTE OU COMPROMETIMENTO**

---

As EC devem estabelecer procedimentos de contingência para as EC e ER subordinadas, estabelecendo as etapas necessárias, de modo a dar continuidade à sua actividade em caso de incidentes, nomeadamente, corrupção ou perda dos dados, software e equipamentos.

Se as EC subcontratarem alguns serviços, as EC garantem que os requisitos anteriores são acautelados e estabelece, obrigatoriamente, um contrato escrito com as provisões necessárias.

As DPC devem descrever os procedimentos adoptados.

---

#### **5.7.2. CORRUPÇÃO DOS RECURSOS INFORMÁTICOS, DO SOFTWARE E/OU DOS DADOS**

---

Se os recursos de hardware, software e/ou dados estão alterados ou há suspeita de terem sido alterados as EC devem suspender os serviços até ao restabelecimento das condições seguras com a inclusão de novos componentes de eficácia credível. A ECEE deve ser notificada.

As DPC devem descrever de forma clara os procedimentos adoptados.

### 5.7.3. PROCEDIMENTOS EM CASO DE COMPROMETIMENTO DA CHAVE PRIVADA DA ENTIDADE

No caso de comprometimento da chave privada de uma entidade, deverá proceder-se à sua revogação imediata e informar deste facto todo o resto das entidades que compõem a SCEE dependentes ou não da Entidade afectada.

Os certificados assinados por entidades dependentes da comprometida, no período compreendido entre o compromisso da chave e a revogação do certificado, deverão por sua vez ser revogados.

No caso de comprometimento da chave de uma EC, o seu certificado é revogado e deve ser gerada nova chave. Dependendo do tipo de EC em causa deverão ser adoptados, no mínimo, os requisitos definidos no quadro seguinte:

ECRAIZESTADO	ECESTADO OU SUBCESTADO
<ul style="list-style-type: none"> <li>- revoga o seu certificado;</li> <li>- emite nova LER;</li> <li>- gera nova chave;</li> <li>- dissemina novo certificado.</li> </ul>	<ul style="list-style-type: none"> <li>- gera um pedido de revogação (CMP);</li> <li>- gera nova chave;</li> <li>- efectua pedido de certificado (PKCS#10);</li> <li>- recebe o novo certificado;</li> <li>- dissemina novo certificado.</li> </ul>
<b>NOTIFICA:</b>	<b>NOTIFICA:</b>
<ul style="list-style-type: none"> <li>- Tutela Política da ECEE</li> <li>- Conselho Gestor;</li> <li>- Outras EC com quem tenha certificação cruzada;</li> <li>- EC subordinadas.</li> </ul>	<ul style="list-style-type: none"> <li>- ECEE</li> <li>- Conselho Gestor;</li> <li>- EC subordinadas e ER;</li> <li>- Todos os titulares.</li> </ul>

Tabela 10 – Procedimentos em caso de comprometimento de chaves

As DPC devem descrever de forma clara os procedimentos adoptados.

---

### **5.7.4. CAPACIDADE DE CONTINUIDADE DA ACTIVIDADE EM CASO DE DESASTRE**

---

As EC devem obrigatoriamente dispor de um plano de continuidade da actividade, onde estão descritos todos os procedimentos a accionar em caso de desastre onde haja perda ou corrupção de dados, software e equipamentos.

O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade de disponibilidade estão disponíveis no Local Alternativo, devendo a DPC indicar o tempo máximo para activação dos serviços.

Nas DPC deverá ser indicado, em caso de indisponibilidade das instalações da EC, o tempo máximo de inactividade antes de ser activado o respectivo Plano de Continuidade da Actividade.

---

### **5.8. PROCEDIMENTOS EM CASO DE EXTINÇÃO DE EC OU ER**

---

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

- a) Informar o Conselho Gestor do SCEE
- b) Informar a Entidade de Certificação Electrónica do Estado;
- c) informar todos os titulares de certificados;
- d) informar as EC com quem tenha efectuado acordos de certificação cruzada (caso existam);
- e) revogar todos os certificados e de certificados cruzados (caso existam);
- f) Efectuar uma notificação final aos titulares 2 (dois) dias antes da cessação formal da actividade;
- g) garantir a transferência (para retenção por outra organização) de toda a informação relativa à actividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

Os arquivos devem ficar sob retenção de acordo com o estipulado no ponto "5.5.2".

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

As DPC devem descrever de forma clara os procedimentos adoptados.

---

## 6. MEDIDAS DE SEGURANÇA TÉCNICAS

---

---

### 6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

---

A geração dos pares de chaves dos vários participantes nesta Infra-estrutura de chaves públicas são processados de acordo com os requisitos e algoritmos definidos nesta política.

---

#### 6.1.1. GERAÇÃO DO PAR DE CHAVES

---

A hierarquia do SCEE prevê a existência de participantes em três níveis.

No primeiro nível, encontra-se a ECRaizEstado, que funciona obrigatoriamente em modo off-line, em que o respectivo par de chaves é gerado num módulo criptográfico, de acordo com requisitos definidos na secção “6.2.1” e o certificado desta entidade é auto-assinado.

No segundo nível, encontra-se as ECEstado, em que o seu funcionamento pode ser efectuado em modo off-line ou em modo on-line (devendo nestes casos obedecer aos requisitos descrito adiante no ponto 6.7). O respectivo par de chaves é gerado, obrigatoriamente, num módulo criptográfico com o nível de protecção adequada, que corresponde aos requisitos definidos no ponto “6.2.1”. O certificado desta entidade é assinado pela ECRaizEstado.

Às entidade de terceiro nível aplicam-se os mesmos requisitos que às entidade de segundo nível.

A geração do par de chaves para o titular é efectuada de acordo com as seguintes condições:

---

##### 6.1.1.1. Chaves para efeitos de Assinatura Digital e Autenticação

---

O processo de geração das chaves é, obrigatoriamente, efectuado directamente num módulo criptográfico em hardware (p.e. *smartcard*), sob o único controlo do titular, não podendo ser feita qualquer cópia da mesma.

O módulo criptográfico, tem obrigatoriamente, um nível de protecção de acordo com o especificado na secção “6.2.1”. Estes certificados são assinados pela EC respectiva.

As DPC devem descrever de forma clara e em pormenor os procedimentos adoptados.

---

##### 6.1.1.2. Chaves para efeitos de Confidencialidade

---

O processo de geração das chaves é, obrigatoriamente, efectuado directamente num módulo criptográfico em hardware (p.e. *smartcard*). O módulo criptográfico, tem obrigatoriamente, um nível de protecção de acordo com o especificado na secção “6.2.1”. Estes certificados são assinados pela EC respectiva.

As DPC devem descrever de forma clara e em pormenor os procedimentos adoptados, em particular se são efectuadas cópias de segurança, como é feita a sua retenção e a sua recuperação, caso seja necessário.

---

### 6.1.2. ENTREGA DA CHAVE PRIVADA AO TITULAR

---

#### 6.1.2.1. Chaves para efeitos de Assinatura Digital e Autenticação

---

A forma de entrega do módulo criptográfico, que contem as chaves, deve ser descrita nas respectivas DPC. No entanto, é obrigatório que a forma de entrega do módulo criptográfico e a forma de entrega do PIN de acesso a este não seja entrega em simultâneo.

#### 6.1.2.2. Chaves para efeitos de Confidencialidade

---

As DPC devem descrever de forma clara e em pormenor os procedimentos adoptados para entrega da chave privada e certificado ao seu titular.

---

### 6.1.3. ENTREGA DA CHAVE PÚBLICA AO EMISSOR DO CERTIFICADO

---

Nos casos em que a entidade emissora do certificado não gera directamente o par de chaves, a sua entrega à EC emissora do certificado deve ser efectuada através de um pedido de certificado (PKCS#10), através de uma transacção on-line (de acordo com o especificado no RFC 2510) ou por outro método igualmente seguro desde que aprovado pelo Conselho Gestor do SCEE.

Os métodos utilizados devem estar descritos nas respectivas DPC.

---

### 6.1.4. ENTREGA DA CHAVE PÚBLICA DA EC ÀS PARTES CONFIANTES

---

A entrega da chave pública da EC, é efectuada pela disponibilização do seu certificado (p.e. no sítio "Web").

Os formatos a disponibilizar podem ser em codificação DER (binário ou base64) ou no formato PKCS#7 (binário ou base64), com ou sem cadeia de certificação, dependendo dos requisitos estabelecidos na respectiva DPC. Outros formatos, para além dos descritos anteriormente, requerem autorização do Conselho Gestor do SCEE.

As DPC devem descrever os métodos utilizados na entrega da chave da EC, bem como os formatos disponibilizados.

---

### 6.1.5. DIMENSÃO DAS CHAVES

---

O que concerne, à dimensão das chaves, os vários participantes devem obedecer aos comprimentos mínimos de chaves:

- a) ECRaizEstado: RSA 4096 bit;
- b) ECEstado: RSA 2048 bit;
- c) subECEstado: RSA 2048 bit;

d) Titulares: RSA 1024 bit.

### 6.1.6. GERAÇÃO DOS PARÂMETROS DA CHAVE PÚBLICA E VERIFICAÇÃO DA QUALIDADE

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo. Em termos exemplificativos, para o caso do algoritmo RSA, deverá ser feita de acordo com o estipulado no PKCS#1 e RFC 3280.

As chaves das EC devem ser geradas com base na utilização de processos aleatórios ou pseudo-aleatórios descritos, respectivamente, na ISO 9564-1 e ISO 11568-5.

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

O campo "*keyUsage*" dos certificados deve ser utilizados de acordo com o recomendado no RFC 3280.

CAMPO "KEYUSAGE" DO CERTIFICADO	BIT ACTIVO
digitalSignature	0
nonRepudiation (contentcommitment)	1
keyEncipherment	2
dataEncipherment	3
keyAgreement	4
keyCertSign	5
cRLSign	6
encipherOnly	7
decipherOnly	8

Tabela 11 – Definição dos campos "Keyusage" dos Certificados SCEE

#### 6.1.7.1. Chaves para efeitos de Assinatura Digital

Este tipo de chaves é utilizado, primordialmente, para efeitos de autenticação, integridade e não-repúdio da informação, devendo ser tido em consideração os seguintes aspectos:

- Quando utilizadas por EC, apenas é permitido que sejam utilizadas para assinar de certificados e CRL (*keyCertSign* e *cRLSign*)
- quando utilizadas pelos titulares, apenas são activadas para não-repúdio (*nonRepudiation - contentcommitment*), de acordo com as recomendações dos

RFC3280 e ETSI 102 280. Não é permitida a presença de outros atributos nos certificados emitidos com este fim

### **6.1.7.2. Chaves para efeitos de Autenticação**

---

Este tipo de chaves é utilizado, primordialmente, para a assinatura digital de e-mail, autenticação em sistemas, etc.

Na prática, estas chaves irão dar suporte às actividades que requerem o uso estendido das chaves.

Deve ser activado o bit "*digitalSignature*", da extensão "*KeyUsage*" do certificado.

### **6.1.7.3. Chaves para efeitos de Confidencialidade**

---

Este tipo de chaves é utilizado, primordialmente, para a troca e estabelecimento de chaves de sessão e processamento da informação cifrada, devendo ser tido em consideração os seguintes aspectos:

Neste tipo de chaves pelo menos um dos seguintes atributos deverá estar presente nos certificados: *keyEncipherment* e/ou *keyAgreement*.

Não é permitida a presença de outros atributos nos certificados emitidos com este fim.

### **6.1.8. OUTRA UTILIZAÇÃO PARA AS CHAVES**

---

Podem ser atribuídas, adicionalmente, outro tipo de utilização das chaves, para além da utilização base descrita anteriormente.

A utilização alargada das chaves apenas é permitida para certificados de titulares (pessoas, organizações ou equipamentos).

A extensão "*extKeyUsage*" pode incluir, os seguintes tipos de utilização:

- a) Server Authentication;
- b) Client Authentication;
- c) CodeSigning;
- d) Email Protection ;
- e) TimeStamping;
- f) OCSPSigning
- g) Smart Card Logon;

## **6.2. PROTECÇÃO DA CHAVE PRIVADA E CARACTERÍSTICAS DO MÓDULO CRIPTOGRÁFICO**

---

Quando for requerida a utilização de módulos criptográficos para protecção das chaves privadas, os participantes desta infra-estrutura deverão empregar dispositivos devidamente avaliados e certificados por organismo e esquema de avaliação adequado para o efeito. O nível de avaliação de segurança requerido para os dispositivos varia em função do nível de protecção requerido e do nível hierárquico que o participante ocupa dentro da infra-estrutura.

---

### **6.2.1. NORMAS E MEDIDAS DE SEGURANÇA DO MÓDULO CRIPTOGRÁFICO**

---

Aos módulos criptográficos utilizados pela ECRaizEstado, ECEstado ou subECEstado, nomeadamente para as operações que dizem respeito à geração, armazenamento e assinatura, é requerida a conformidade e respectiva certificação em pelo menos uma das seguintes normas (ou critérios reconhecidos como equivalentes):

- a) FIPS PUB 140-2 com nível 3 ou superior;
- b) CWA 14167-2;
- c) ISO/IEC 15408 em EAL 4 ou superior.

Quando está em causa uma EREstado, os requisitos expressos anteriormente, referem-se às chaves do sistema /administrador da mesma.

Aos titulares de certificados é requerida a utilização de módulos criptográficos certificados segundo o padrão ISO/IEC 15408 EAL4+ com suporte às normas PKCS#11 e CSP.

---

### **6.2.2. CONTROLO MULTI-PESSOAL (N DE M) PARA A CHAVE PRIVADA**

---

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

Todas as operações deverão ser efectuadas com um mínimo de 2 pessoas (com funções qualificadas dentro da entidade) por tarefa, sendo empregues nas diversas funções, pelo menos 2 pessoas (N=2), entre o conjunto total de pessoas com funções atribuídas dentro da entidade (M=staff).

As DPC deverão descrever de forma precisa o número de pessoal empregue por tarefa.

---

### **6.2.3. RETENÇÃO DA CHAVE PRIVADA (KEY ESCROW)**

---

Não é autorizada a retenção de chaves privadas para efeitos de assinatura digital.

Esta autorizado a retenção de chaves privadas para efeitos de confidencialidade. Nos procedimentos para recuperação deste tipo de chaves, é requerido controlo multi-pessoal.

As DPC deverão descrever de forma precisa os mecanismos utilizados.

---

### **6.2.4. CÓPIA DE SEGURANÇA DA CHAVE PRIVADA**

---

As chaves privadas dos titulares, para efeitos de assinatura digital, não são alvo de qualquer cópia de segurança.

As chaves privadas das Entidades Certificadoras do SCEE deverão ser alvo, obrigatoriamente, de pelo menos uma cópia de segurança, a realizar pela própria entidade. As cópias de segurança deverão ter o mesmo nível de segurança que a chave original.

---

### **6.2.5. ARQUIVO DA CHAVE PRIVADA**

---

Todas as chaves que tenham sido alvo de cópias de segurança, deverão ser arquivadas de acordo com o estabelecido na secção “5.5.2”.

---

### **6.2.6. TRANSFERÊNCIA DA CHAVE PRIVADA PARA/DO MÓDULO CRIPTOGRÁFICO**

---

No caso das chaves com utilização para efeitos de assinatura digital a transferência de e para o módulo criptográfico não se aplica, uma vez que são geradas dentro deste.

Assim esta situação não é aplicável para as chaves das EC, nem para as chaves de titulares, quando utilizadas para efeitos de assinatura digital.

No caso das chaves com utilização para efeitos de confidencialidade, se estas não forem geradas dentro do módulo criptográfico, a forma de a transferir deverá ser efectuada de acordo com o descrito no RFC 2510.

---

### **6.2.7. ARMAZENAMENTO DA CHAVE PRIVADA NO MÓDULO CRIPTOGRÁFICO**

---

As chaves das EC são geradas e guardadas em módulo criptográfico de acordo com o especificado na secção “6.2.1”.

---

### **6.2.8. PROCESSO PARA ACTIVAÇÃO DA CHAVE PRIVADA**

---

A chave privada deverá ser activada quando o sistema quando o sistema/aplicação da EC é ligado (“*startup process*”). Esta activação só deverá ser efectivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos indivíduos indicados para o efeito.

O mecanismo de autenticação mínimo exigido é a autenticação por PIN/ palavra-chave. O número máximo de tentativas de autenticação permitidas não deve ser superior a 5 tentativas.

As DPC deverão descrever o procedimento utilizado para activação da chave privada, bem como a identificação e interacção das pessoas com o sistema/aplicação/módulo criptográfico durante o processo.

---

### **6.2.9. PROCESSO PARA DESACTIVAÇÃO DA CHAVE PRIVADA**

---

A chave privada deverá ser desactivada quando o sistema quando o sistema/aplicação da EC é desligado (“*shutdown process*”). Esta desactivação só deverá ser efectivada quando previamente tiver sido encerrada a sessão com o módulo criptográfico.

Neste processo, antes de finalizado, deve ser garantido que todas as chaves são eliminadas da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave tenha sido eventualmente armazenada, deve ser reescrito

As DPC deverão descrever o procedimento utilizado para desactivação da chave privada, bem como a identificação e interacção das pessoas com o sistema/aplicação/módulo criptográfico durante o processo.

---

### 6.2.10. PROCESSO PARA DESTRUIÇÃO DA CHAVE PRIVADA

---

As várias chaves privadas devem ser destruídas sempre que deixarem de ser necessárias. De forma geral, esta actividade deve ser precedida sempre pela revogação do certificado, no caso de estar em vigor.

Para além do descrito no ponto anterior (6.2.9), as respectivas cópias de segurança devem também ser alvo de destruição.

A destruição das chaves privadas podem passar por processos diversos, consoante se enquadrem nos casos descritos a seguir:

- a) **sem formatação do modulo criptográfico:** Nas situações renovação de chaves (de rotina), a destruição da chave privada antiga é efectuada reescrevendo a nova chave privada do titular.
- b) **com formatação do modulo criptográfico:** Nas situações em a chave privada deixou de poder ser utilizada, nomeadamente, após expiração ou revogação do certificado.
- c) **destruição física:** Sempre que existam modulo criptográficos personalizados, nomeadamente "*smartcards*" com fotografia. Antes da sua destruição física, devem ser previamente formatados.

Todos os procedimentos relativos à destruição das chaves privadas, bem como a gestão do ciclo de vida dos módulos criptográficos personalizados devem estar descritos nas respectivas DPC

---

### 6.2.11. AVALIAÇÃO/NÍVEL DO MÓDULO CRIPTOGRÁFICO

---

Descrito no ponto 6.2.1

---

## 6.3. OUTROS ASPECTOS DA GESTÃO DO PAR DE CHAVES

---

---

### 6.3.1. ARQUIVO DA CHAVE PÚBLICA

---

As EC devem efectuar o arquivo das suas chaves e das chaves por si emitidas (para efeitos de assinatura digital), permanecendo armazenadas após a expiração dos certificados correspondentes, de acordo com os requisitos definidos no ponto 5.5, para verificação de assinaturas geradas durante seu prazo de validade.

### 6.3.2. PERÍODOS DE VALIDADE DO CERTIFICADO E DAS CHAVES

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

Neste sentido a tabela seguinte apresenta a validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados. Os valores estão expressos em anos.

[VALIDADE DOS CERTIFICADOS] – [PERÍODO DE RENOVAÇÃO]					
ECRaizEstado	ECEstado	subECEstado	Outras Entidades PKI	Titulares	
				Hardware	Software
[24] – [12]	[12] – [6]	[6] – [3]	[3] – [3]	[3] – [3]	[1] – [1]

Outras Entidades PKI: EREstado, Serviços de Validação Cronológica e Serviços de Validação On-line do Estado de Certificados

Tabela 12 – Definição dos Períodos de Validade dos Certificados

### 6.4. DADOS DE ACTIVAÇÃO

#### 6.4.1. GERAÇÃO E INSTALAÇÃO DOS DADOS DE ACTIVAÇÃO

Os dados de activação devem ser gerados de forma a serem únicos e imprevisíveis. Os dados de activação conjugados com outro tipo de controlo de acessos, deve ter um adequado nível de robustez para as chaves e dados a proteger.

A entrada de uma EC no domínio da SCEE, requer a existência de dispositivos/mecanismos criptográficos (p.e. *smartcards*) para suporte às actividades das EC, nomeadamente no seu funcionamento e na sua recuperação.

A actividade das EC é efectuada com base em funções diferenciadas, cada uma com o correspondente dispositivo onde se encontram os respectivos dados de activação.

#### 6.4.2. PROTECÇÃO DOS DADOS DE ACTIVAÇÃO

Apenas o pessoal autorizado tem em posse os dispositivos (p.e. *Smartcard*, PED, etc.) e respectivo segredo (p.e. PIN) dos dados de activação das EC.

No caso de chaves associadas a certificados de titulares, apenas o próprio conhece o respectivo segredo para activação, sendo este o único e exclusivo responsável pela protecção e guarda dos dados de activação das suas chaves.

### **6.4.3. OUTROS ASPECTOS DOS DADOS DE ACTIVACÃO**

---

Não estipulado.

### **6.5. MEDIDAS DE SEGURANÇA INFORMÁTICA**

---

Os dados relativos a esta secção são considerados sensíveis, sendo apenas disponibilizados a quem tiver necessidade de conhecer. No domínio da SCEE, apenas são fornecidos à Entidade de Certificação Electrónica do Estado, ao Conselho Gestor do SCEE e a Autoridade Credenciadora.

Cada EC deve implementar o conjunto de medidas de segurança consideradas adequadas, em resultado da arquitectura escolhida e dos riscos avaliados.

As DPC devem conter uma descrição das medidas de segurança implementadas, sem colocar em causa a segurança dos sistemas por eventual excesso de divulgação de informação.

#### **6.5.1. REQUISITOS TÉCNICOS ESPECÍFICOS**

---

De forma geral os sistemas que compõe a EC devem proporcionar, desde que aplicável, no mínimo, as seguintes capacidades/funcionalidades:

- a) As descritas no ponto 5, do documento “CWA 14167-1”;
- b) mecanismos para recuperação dos sistemas e chaves de EC;
- c) dispositivos de protecção de fronteira, nomeadamente, firewall, IDS/IPS.

Os requisitos definidos anteriormente, devem ser alcançados pela conjunção dos diversos sistemas que compõem os sistemas seguro da EC (p.e. sistema operativo, software, HSM, medidas de segurança física, etc.).

Outros tipos de software (p.e. antivírus,), só deve ser instalado se for verificados que:

- a) não interfere com as configurações previamente definidas pelos fabricantes/organismos de avaliação; e
- b) se demonstrar que proporciona um acréscimo no nível de segurança.

De modo general as EC devem seguir as boas práticas estabelecidas na norma ISO 17799:2005.

#### **6.5.2. AVALIAÇÃO/NÍVEL DE SEGURANÇA**

---

Os vários sistemas e produtos empregues pelas EC, no domínio da SCEE, são fiáveis e protegidos contra modificações. Os produtos e sistemas referidos, são avaliados, estando em conformidade com os requisitos definidos na especificação técnica CWA 14167-1 e/ou com a norma ISO 15408 ou perfil equivalente.

---

### **6.6. CICLO DE VIDA DAS MEDIDAS TÉCNICAS DE SEGURANÇA**

---

Os dados relativos a esta secção são considerados sensíveis, sendo apenas disponibilizados a quem tiver necessidade de conhecer. No domínio da SCEE, apenas são fornecidos à ECEE, ao Conselho Gestor do SCEE e a Autoridade Credenciadora.

Cada EC deve implementar o conjunto de medidas de segurança consideradas adequadas, em resultado da arquitectura escolhida e dos riscos avaliados.

As DPC devem conter uma descrição das medidas de segurança implementadas, sem colocar em causa a segurança dos sistemas por eventual excesso de divulgação de informação.

---

#### **6.6.1. MEDIDAS DE DESENVOLVIMENTO DO SISTEMA**

---

São exigidos requisitos de segurança desde o início, na aquisição dos sistemas informáticos como no instalação e implementação dos mesmos, visto que podem ter algum impacto sobre a segurança da SCEE.

Serão realizadas análises dos requisitos de segurança durante as fases de desenho e especificação de requisitos de qualquer componente utilizado nas aplicações que constituem cada um dos sistemas da SCEE, para garantir que os sistemas são seguros.

Utilizam-se procedimentos de verificação de alteração de versões, actualizações e instalação de patches ou *fixes* dos ditos componentes.

A infra-estrutura das ECs deve estar dotadas de ambientes de desenvolvimento e pré-produção segregados dos ambientes de produção.

---

#### **6.6.2. MEDIDAS PARA A GESTÃO DA SEGURANÇA**

---

A EC deve manter actualizado um inventário com todos os activos (equipamento, dados e pessoal), sendo classificados de acordo com a sua importância e necessidades de protecção, tendo em conta o normal funcionamento da actividade da EC. Esta classificação deve estar coerente com a análise de riscos inicial.

De modo geral as EC devem regular a sua actividade pela adopção dos seguintes princípios:

- a) Os produtos e sistemas da EC devem única e exclusivamente ser utilizados para as actividades de certificação;
- b) A configuração dos produtos e sistemas da EC, tal como a sua manutenção devem ser sempre documentadas;
- c) Nos sistemas das EC apenas deve ser instalado aplicações e componentes indispensáveis para o seu funcionamento;
- d) Devem estar previstos mecanismo para detecção de eventuais modificações na sua configuração;
- e) Devem ser adoptadas medidas adequadas para a prevenção de software malicioso

carregado através dos equipamentos das ER;

- f) Depois de instalado, os sistemas e produtos da EC devem efectuar verificações da sua integridade, de forma periódica, nunca ultrapassando, o período de 30 dias entre verificações.

A DPC deve descrever a medidas adoptadas, com um detalhe que não coloque em causa a segurança do sistema.

---

### 6.6.3. CICLO DE VIDA DAS MEDIDAS DE SEGURANÇA

---

As operações de actualização e manutenção dos produtos e sistemas das EC, devem seguir o mesmo controlo que o equipamento original e deve ser instalado pelo pessoal com funções de confiança, com adequada formação para o efeito, seguindo os procedimentos definidos para o efeito.

Nas DPC devem estar descritos os procedimentos a seguir para a actualização e manutenção dos produtos e sistemas que compõe o sistema da EC.

---

### 6.7. MEDIDAS DE SEGURANÇA DA REDE

---

Os sistemas da EC que se encontrem a funcionar em modo *on-line* devem estar protegidos de eventuais ataques em virtude de estarem interligados, directa ou indirectamente, a redes externas. Esta protecção deve ser garantida com o recurso a equipamentos de protecção de fronteira, nomeadamente, um *Firewall*, configurado de forma a permitir apenas a utilização de protocolos e comandos necessários para o correcto funcionamento do sistema da EC responsável pela emissão dos certificados.

**A DPC deve descrever a medidas de segurança de rede adoptadas, com um detalhe que não coloque em causa a segurança do sistema.**

---

### 6.8. VALIDAÇÃO CRONOLÓGICA (TIME-STAMPING)

---

As EC integradas na infra-estrutura de chave pública da SCEE, asseguram que a data e a hora incluída em todas as fases do ciclo de vida do certificado, são determinadas através de uma fonte de tempo segura, nomeadamente, a do Observatório Astronómico de Lisboa.

Os dados relacionados com a geração e a gestão das chaves utilizadas na validação cronológica, incluindo os dados associados à certificação da hora por um instituto nacional de medida, são registados e arquivados por um período mínimo de 20 anos.

Neste contexto, os serviços de validação cronológica, associam com recurso a mecanismos e protocolos baseados em criptografia de chave pública os dados e o tempo, garantindo em todo o momento que:

- a) A origem e a validade de cada pedido de validação cronológica são conhecidas;
- b) O pedido utiliza um algoritmo criptográfico aprovado pelo Conselho Gestor do SCEE;
- c) É utilizada a hora UTC, certificada pelo OAL, com incerteza inferior a 100 milissegundos;

- d) Os dados incluídos no pedido são devolvidos garantindo a sua integridade, sem alteração ou modificação;
- e) A chave privada utilizada na assinatura da prova de validação cronológica:
  - f) Apenas é utilizada para esse fim;
  - g) Utiliza um algoritmo criptográfico aprovado pelo Conselho Gestor do SCEE;
  - h) É gerada e armazenada num módulo criptográfico, de acordo com as especificações definidas no ponto 6.2.1;
  - i) Em cada prova de validação cronológica são incluídos:
    - j) O valor tempo certificado;
    - k) Um identificador único;
    - l) Um indicador único da política de certificação cronológica adoptada;
  - m) O grau de exactidão do valor tempo utilizado sempre que aquele seja superior ao indicado na política adoptada;
- n) A prova de validação cronológica é assinada criptograficamente antes da devolução da resposta ao pedido;
- o) Não está incluída, na prova de validação cronológica, a identificação da entidade que a solicitou.

---

## 7. PERFIS DE CERTIFICADO, CRL E OCSP

---

---

### 7.1. PERFIL DO CERTIFICADO

---

A emissão de certificados é feita segundo o perfil de Certificados ITU-T X.509 versão 3, de acordo, com as recomendações definidas no RFC 3280, RFC 3739, ETSI TS 101 862 e ETSI 102 280.

Os certificados emitidos pelas EC, no domínio da SCEE, devem incluir,;

CAMPO	DESCRIÇÃO
serialNumber	numero inteiro que indica o número de série do certificado;
signature	OID do algoritmo utilizado pela EC para assinar o certificado;
issuer	um X.500 DN da EC que emite o certificado
validity	o período de tempo em que o certificado é considerado válido.
	nos certificados até 2049: representado num "UTC Time" (YYMMDDHHMMSSZ).
	nos certificados após 2049: representado num "generalized time" (YYYYMMDDHHMMSSZ).
subject	um X.500 DN a quem é atribuído o certificado
subjectPublicKeyInfo	OID do algoritmo e uma cópia da chave publica do certificado

Tabela 13 – Campos básicos do certificado

---

#### 7.1.1. NÚMERO(S) DE VERSÃO

---

Neste campo os certificados deverão conter o valor 2 (dois), de forma a identificar a utilização de certificados ITU-T X.509 versão 3.

---

#### 7.1.2. EXTENSÕES DO CERTIFICADO

---

Todos os sistemas das várias entidades deverão processar correctamente todas as extensões identificadas no RFC 3280.

---

##### 7.1.2.1. authorityKeyIdentifier

---

Extensão obrigatória e não critica. Esta extensão é utilizada para verificar a assinatura do certificado, possibilitando que as várias chaves utilizadas pelas EC na assinatura dos certificados, sejam facilmente diferenciadas. O valor do "keyIdentifier" deve derivar da chave pública da EC (normalmente um hash da chave pública que consta no campo "subjectPublicKeyInfo" do certificado da EC que o emitiu).

Nos certificados auto-assinados não é utilizado.

### 7.1.2.2. subjectKeyIdentifier

---

Extensão obrigatória e não crítica. Esta extensão é utilizada para identificar de forma inequívoca a chave pública do certificado. Possibilita que várias chaves sejam utilizadas pelo mesmo “subject” e que sejam facilmente diferenciadas. O valor utilizado é normalmente um hash da chave pública que consta no campo do certificado “subjectPublicKeyInfo”.

### 7.1.2.3. KeyUsage

---

Extensão obrigatória e crítica. Especificado na secção 6.1.7 deste documento.

### 7.1.2.4. certificatePolicies

---

Extensão obrigatória e não crítica. Esta extensão lista as Políticas de Certificados que dão suporte e regem o ambiente em que se processou a emissão do certificado. Deve ser incluído o OiD da Política de Certificado e o URL da DPC.

### 7.1.2.5. BasicConstraints:

---

É uma extensão obrigatória e crítica para Certificados de EC, é opcional para certificados de titular. Se o certificado é um certificado de EC, o valor “cA”, deverá estar activo (cA=True).

Em termos práticos, se num certificado o campo “keyUsage” estiver presente o valor “keyCertSign”, então no *BasicConstraints*, o valor do campo “cA”, deverá ser estar activo, ou o processo de verificação do certificado falha.

### 7.1.2.6. Authority Information Access

---

A extensão “Authority Information Access”, é introduzida nos vários perfis de certificados definidos no âmbito da SCEE, de forma a permitir futuras implementações para verificação via OSCP, sem que para isso haja necessidade de futuras alterações nesta infra-estrutura de chaves públicas

---

## 7.1.3. IDENTIFICADORES DE ALGORITMO

---

ALGORITMO	OID
Sha1WithRSAEncryption	1.2.840.113549.1.1.5
Sha256withRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tabela 14 – Identificadores OiD de Algoritmos

---

### 7.1.4. FORMATOS DE NOME

---

Os Certificados emitidos para cada entidade do SCEE são referenciados através de um DN, a aplicar nos campos “*issuer*” e “*subject*” do certificado.

Os DN deverão ser representados através de uma *X.501 UTF8String*.

---

### 7.1.5. RESTRIÇÕES DE NOME

---

Os nomes incluídos nos certificados estão restritos à utilização de DN, únicos e sem ambiguidades.

O atributo “C” (countryName) é codificado de acordo com a ISO 3166-1-alpha-2 code elements”, numa *PrintableString*.

---

### 7.1.6. OBJECTO IDENTIFICADOR DA POLÍTICA DE CERTIFICADO

---

Todos os certificados emitidos pelas Entidades Certificadoras do SCEE devem garantir a inclusão do OID da Política de certificado

---

### 7.1.7. UTILIZAÇÃO DA EXTENSÃO DE RESTRIÇÃO DE POLÍTICAS

---

Nada a assinalar.

---

### 7.1.8. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICAS

---

Nos certificados emitidos, as Entidades Certificadoras devem incluir no campo *policyQualifiers* da extensão “*CertificatePolicies*” o URL da sua DPC.

Nas DPC poderão ser estabelecidos a utilização do ‘*Policy Qualifier*’, o campo ‘*Notice Referencé*’. O ‘*Notice Referencé*’, é uma nota de texto que aparece no monitor, quando se procede a verificação do certificado.

---

### 7.1.9. SEMÂNTICA DE PROCESSAMENTO DA EXTENSÃO DE POLÍTICA DE CERTIFICADOS CRÍTICOS

---

Tendo em consideração as recomendações introduzidas pelo RFC 3280, quanto à utilização desta extensão, os certificados das EC do SCEE devem incluir no OiD o valor 2.5.29.32.0.

Esta opção tem como objectivo não limitar, em termos futuros, o conjunto de políticas a emitir sob o domínio de certificação da SCEE.

Nos certificados para titulares serão incluídos os OiD respectivo, tendo em conta a sua aplicação.

Esta extensão é marcada como não critica para evitar problemas de interoperabilidade.

### 7.2. PERFIL DA LCR

Cada EC da SCEE, na emissão de uma LCR, deve obrigatoriamente incluir:

CAMPO	DESCRIÇÃO
signature	OID do algoritmo utilizado pela EC para assinar o certificado; o algoritmo e respectivo OID
issuer	um X.500 DN da EC que emite o certificado o X.500 DN da EC que gerou a LCR;
thisUpdate	a indicação de quando a LCR foi gerada
nextUpdate	a indicação de quando será gerada nova LCR
revokedCertificates	deverá ser introduzida a sequência de dados correspondentes aos campos <i>userCertificate</i> , <i>revocationDate</i> e <i>crEntryExtensions</i> , de forma a fornecer informação do estado dos certificados no que diz respeito, respectivamente, ao número de série do certificado revogado, a data em que foi revogado e o motivo da sua revogação

Tabela 15– Campos básicos do certificado

Adicionalmente, as diversas aplicações e sistemas utilizados pelos participantes que integram a SCEE, devem garantir, entre outras que:

- A verificação da assinatura constante na LCR, através da chave pública constante no certificado da EC que emite a LCR;
- Verificar a cadeia de certificação do certificado da EC;
- Verificar que é utilizada a versão 2;
- No momento da verificação a data está enquadrada de acordo com os valores indicados nos campos da LCR “*thisUpdate*” e “*nextUpdate*”;
- A LCR que está a ser verificada, no seu campo “*CRLNumber*”, o valor indicado é superior ao valor constante no mesmo campo da LCR já existente;
- Que a entidade que emite a LCR é a mesma que emitiu o certificado;

#### 7.2.1. NÚMERO(S) DA VERSÃO

As CRL emitidas pelas EC, devem implementar versão 2 padrão ITU X.509, de acordo com o RFC 3280

### 7.2.2. EXTENSÕES DA CRL E DAS SUAS ENTRADAS

---

A SCEE define como extensões de CRL obrigatórias, não críticas, as seguintes:

- g) CRLNumber, implementado de acordo com as recomendações do RFC 3280;
- h) AuthorityKeyIdentifier: contem um identificador da chave pública da EC que assinou a LCR;

### 7.3. PERFIL DO OCSP

---

Se o serviço de OCSP for implementado, os certificados de OCSPResponder, devem estar em concordância com as seguintes normas:

- a) RFC 3280;
- b) ITU-T X.509 (2005);
- c) RFC 2560.

E tendo em conta os seguintes constrangimentos:

- a) O período de validade não deve ser superior a 6 meses.
- b) No certificado de OCSP será incluída a extensão “*id-pkix-ocsp-nocheck*”.

No entanto, de futuro não deve ser excluída a possibilidade de inclusão da extensão AIA, fornecendo informação sobre os mecanismos adicionais para comprovação da validade dos certificados.

#### 7.3.1. NÚMERO(S) DA VERSÃO

---

Os certificados de *OCSP Responder* utilizam a norma X.509 versão 3 (X.509 v3).

#### 7.3.2. EXTENSÕES DO OCSP

---

Os certificados de OCSP Responder emitidos por uma EC no domínio do SCEE incluirão o DN da entidade emissora e do titular, nos campos “*issuer name*” e “*subject name*”, respectivamente.

Os campos e extensões utilizadas nos certificados de OCSP Responder são:

- a) Version;
- b) serialNumber;
- c) subject;
- d) issuer;
- e) signingAlgorithms;
- f) validityPeriod;
- g) extKeyUsage;
- h) subjectKeyIdentifier;

- i) authorityKeyIdentifier issuerAndSerialPresent;
- j) KeyUsage, marcada como crítica;
- k) BasicConstraint, marcada como crítica;
- l) CertificatePolicies;
- m) OCSPNocheck;
- n) AIA;

---

## **8. AUDITORIA E AVALIAÇÕES DE CONFORMIDADE**

---

Todas as EC integradas na hierarquia da SCEE, devem obrigatoriamente, construir as suas DPC em conformidade com os requisitos mínimos definidos neste documento.

São alvo de auditoria todas as entidades que directa ou indirectamente exerçam actividade de certificação nos termos do definido nesta politica, como são o caso da ECRaizEstado, das ECEstado e das subECEstado e EREstado, caso existam.

A Autoridade Credenciadora é o organismo responsável pela condução das auditorias de conformidade, podendo recorrer a pessoal externo.

---

### **8.1. FREQUÊNCIA OU MOTIVO DA AUDITORIA**

---

De acordo com o descrito no ponto 8, as diversas entidades são alvo de auditoria nas seguintes situações:

- a) No processo de integração na SCEE;
- b) Anualmente; e
- c) A qualquer momento, sem aviso prévio.

As EC do Estado devem declarar na DPC a frequência das auditorias, sendo que estas devem ser realizadas pelo menos uma vez por ano, de forma a garantir a adequação do funcionamento e operação de acordo com a DPC.

Podem ser levadas a cabo outras auditorias técnicas e de segurança segundo o estabelecido nas DPC.

Cada EC deverá efectuar com uma regularidade a explicitar, auditorias de cumprimento de legislação e de protecção de dados pessoais

---

### **8.2. IDENTIDADE E QUALIFICAÇÕES DO AUDITOR**

---

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 chaves pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança.

A Autoridade Credenciadora é responsável pela selecção e nomeação do pessoal que realiza a auditoria.

O auditor 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 sistema de informação
- b) Independência a nível orgânico da Entidade Certificadora (para os casos de auditorias externas)

**Deve ser credenciado pelo Gabinete Nacional de Segurança**

---

### **8.3. RELAÇÃO ENTRE O AUDITOR E A ENTIDADE CERTIFICADORA**

---

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

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

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

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

---

### **8.4. ÂMBITO DA AUDITORIA**

A auditoria de segurança é efectuada com base nos requisitos mínimos definidos neste documento e na DPC da entidade que irá ser alvo da auditoria.

As auditorias determinam a conformidade dos serviços das EC do Estado com estas Políticas de Certificados e com as Declarações de Práticas. Também devem determinar a adequação referente aos seguintes documentos:

- a) Política de Segurança
- b) Segurança Física
- c) Avaliação Tecnológica
- d) Gestão dos serviços da EC
- e) Selecção de Pessoal
- f) DPC e PC (em vigor)
- g) Contratos
- h) Política de Privacidade

As auditorias podem ser completas ou parciais, incidir sobre qualquer outro tipo de documentos / procedimentos, tendo em consideração os critérios definidos no CWA 14172-2

---

### **8.5. PROCEDIMENTOS APÓS UMA AUDITORIA COM RESULTADO DEFICIENTE**

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

- a) Documenta todas as deficiências encontradas durante a auditoria;
- b) No final da auditoria reúne com os responsáveis da entidade submetida a auditoria e apresenta de forma resumida um relatório de primeiras impressões (RPI);
- c) Elabora o relatório auditoria. Este relatório deverá estar organizado de modo a que todas as deficiências sejam escalonadas por ordem decrescente de gravidade/severidade;
- d) Submete o relatório de auditoria à Entidade de Certificação Electrónica do Estado e ao Conselho Gestor do SCEE para apreciação;
- e) Depois de apreciado e consolidado, é remetida uma cópia do relatório de auditoria

final (RAF), para a entidade;

- f) Tendo em conta a irregularidades constantes no relatório, a entidade submetida à auditoria enviará uma relatório de correcção de irregularidades (RCI), para a ECEE, no qual deve estar descrito quais as acções, metodologia e tempo necessário para corrigir as irregularidades encontradas;
- g) A Entidade de Certificação Electrónica do Estado obtém parecer consultivo do Conselho Gestor e em conjunto com a Autoridade Credenciadora depois de analisar este relatório tomam uma das três seguintes opções, consoante o nível de gravidade/severidade das irregularidades:
- i. Aceitam os termos, permitindo que a actividade seja desenvolvida até à próxima inspecção;
  - ii. Permitem que a entidade continue em actividade por um período máximo de 60 dias até à correcção das irregularidades antes da revogação;
  - iii. Revogação imediata da actividade.

### 8.6. COMUNICAÇÃO DE RESULTADOS

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

COMUNICAÇÃO DE RESULTADOS	AUDITOR	ENTIDADE	ECEE
RPI	No final da auditoria		
RAF	2 semanas		
RCI		1 semana	
Decisão sobre irregularidades			4 semanas

Tabela 16 – Prazos de comunicação dos resultados de Auditoria

---

## **9. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS**

---

---

### **9.1. TAXAS**

---

---

#### **9.1.1. TAXAS POR EMISSÃO OU RENOVAÇÃO DE CERTIFICADOS**

---

As taxas de emissão ou renovação de certificados se existirem, devem estar detalhadas na DPC.

---

#### **9.1.2. TAXAS PARA ACESSO A CERTIFICADO**

---

De forma geral, da a natureza pública de que se reveste a SCEE, o acesso será tendencialmente gratuito, no entanto, a EC deve descrever a sua aplicabilidade na sua DPC.

---

#### **9.1.3. TAXAS PARA ACESSO A INFORMAÇÃO DO ESTADO CERTIFICADO OU DE REVOGAÇÃO**

---

O acesso a informação sobre o estado ou revogação dos certificados é livre e gratuita não se podendo aplicar nenhuma taxa.

---

#### **9.1.4. TAXAS PARA OUTROS SERVIÇOS**

---

De forma geral, da a natureza pública de que se reveste a SCEE, o acesso será tendencialmente gratuito, no entanto, a EC deve descrever a sua aplicabilidade na sua DPC.

---

#### **9.1.5. POLÍTICA DE REEMBOLSO**

---

Nos casos em que a DPC especifique alguma taxa aplicável à prestação de serviços de certificação ou revogação para determinado tipo de certificados, é obrigatório que esse documento especifique a Política de reembolso.

---

## **9.2. RESPONSABILIDADE FINANCEIRA**

---

---

### **9.2.1. SEGURO DE COBERTURA**

---

As Entidade Certificadoras do Estado, devem respeitar a legislação em vigor no que se concerne aos seguros de cobertura de responsabilidade civil, devendo identificar nas respectivas Declarações de Práticas o montante e a cobertura.

---

### **9.2.2. OUTROS RECURSOS**

---

Como as Entidades Certificadoras do SCEE pertencem ao Estado Português, não estão sujeitas aos riscos inerentes às Entidade Certificadoras Privadas.

### **9.2.3. SEGURO OU GARANTIA DE COBERTURA PARA UTILIZADORES**

---

Existindo seguro de ou garantia de Cobertura para Utilizadores, as EC devem especifica-los na DPC.

### **9.3. CONFIDENCIALIDADE DA INFORMAÇÃO PROCESSADA**

---

O pedido de inclusão no certificado de dados pessoais da pessoa singular a constar como seu titular terá de ser expressamente autorizado pela própria.

#### **9.3.1. ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO**

---

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

- a) As chaves privadas das Entidades que compõem a SCEE;
- b) As chaves privadas dos titulares da SCEE;
- c) Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
- d) Toda a informação de carácter pessoal proporcionada às EC 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;

#### **9.3.2. INFORMAÇÃO FORA DO ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO**

---

Considera-se informação de acesso público:

- a) Política de Certificados
- b) Declaração de Práticas de Certificação
- c) Os certificados para efeitos de confidencialidade, desde que declarado na respectiva DPC;
- d) LCR e LER;
- e) Toda a informação classificada como “pública”

As Entidades Certificadoras devem permitir o acesso a informação não confidencial sem prejuízo do que se venha a estabelecer nas DPC nos controles de segurança necessários para proteger a autenticidade e integridade da mesma.

#### **9.3.3. RESPONSABILIDADE DE PROTECÇÃO DA CONFIDENCIALIDADE DA INFORMAÇÃO**

---

Deve ser declarado na DPC a responsabilidade de protecção da confidencialidade da informação.

---

### 9.4. PRIVACIDADE DOS DADOS PESSOAIS

---

As Entidades Certificadoras devem ter uma Política de Privacidade nos seus repositórios, onde se declara o cumprimento das disposições estabelecidas na legislação de protecção de dados pessoais, tendo em consideração que:

- a) As EC só podem coligir dados pessoais necessários ao exercício das suas actividades e obtê-los directamente das pessoas interessadas na titularidade dos dados de criação e verificação de assinatura e respectivos certificados, ou de terceiros junto dos quais aquelas pessoas autorizem a sua colecta;
- b) Os dados pessoais coligidos pela EC não poderão ser utilizados para outra finalidade que não seja a de certificação, salvo se outro uso for consentido expressamente por lei ou pela pessoa interessada;
- c) As EC respeitarão as normas legais vigentes sobre a protecção, tratamento e circulação dos dados pessoais e sobre a protecção da privacidade no sector das telecomunicações.

---

#### 9.4.1. MEDIDAS PARA GARANTIA DA PRIVACIDADE

---

No cumprimento do estabelecido pela lei sobre assinaturas electrónicas, informação de carácter pessoal disponibilizada às EC do Estado pelos titulares de certificados, deve ser tratada de acordo com a lei de protecção de dados pessoais.

Desta forma cada DPC deve declarar a existência de um ficheiro de dados utilizadores de assinaturas electrónicas, indicando a responsabilidade do mesmo e a autorização da CNPD.

---

#### 9.4.2. INFORMAÇÃO PRIVADA

---

A informação pessoal que não incluída nos certificados, bem como o mecanismo de comprovação do estado dos certificados, devem ser considerados informação de carácter privado. Em qualquer caso são exemplos de informação considerada privada:

- a) Pedidos de certificados, aprovados ou negados assim como toda a informação pessoal obtida para a emissão e manutenção de certificados;
- b) Chaves privadas geradas e/ou armazenadas pelas EC da SCEE
- c) Os dados pessoais a que se refere a Lei 67/98

Em nenhum caso as EC do Estado poderão incluir nos certificados que emitem, os dados que se faz referência no artigo 7 da Lei 67/98.

### **9.4.3. INFORMAÇÃO NÃO PROTEGIDA PELA PRIVACIDADE**

---

Esta informação é referente à informação pessoal que se inclui no certificados e no mecanismo de comprovação do estado dos mesmos de com a secção 3.1 deste Documento.

Esta informação, proporcionada aquando do pedido de certificado é incluída nos certificados.

Esta informação não tem carácter privado / reservado, sendo deste modo pública caso seja consentido pelo titular.

Em todo o caso não é considerada confidencial a seguinte informação:

- a) O período de validade do certificado assim como a data de emissão do certificado e a data de caducidade;
- b) O número de série do certificado;
- c) Os diferentes estados e situações do certificado e a data do início de cada um deles;
- d) As lista de revogação de certificados (CRL) assim como o resto das informação de estado de revogação;
- e) A informação contida no Repositório das EC.

### **9.4.4. RESPONSABILIDADE DE PROTECÇÃO DA INFORMAÇÃO PRIVADA**

---

As EC devem garantir o cumprimento das suas obrigações, como previsto neste documento.

### **9.4.5. NOTIFICAÇÃO E CONSENTIMENTO PARA UTILIZAÇÃO DE INFORMAÇÃO PRIVADA**

---

Para a prestação de serviço, as EC deverão obter o consentimento dos titulares dos dados necessários para a prestação do serviço de certificação. Considera-se obtido o consentimento por parte do titular a oposição da assinatura do TRT.

### **9.4.6. DIVULGAÇÃO RESULTANTE DE PROCESSO JUDICIAL OU ADMINISTRATIVO**

---

As EC só poderão fornecer dados e informações consideradas, no âmbito desta política, como informação privada, nos pressupostos em que estes são requeridos pela autoridade pública competente no âmbito da lei vigente.

Em concreto, as EC estão obrigadas a revelar a identidade dos assinantes quando lhes for solicitado pelos órgãos judiciais no exercício das funções que lhe sejam atribuídas.

### **9.4.7. OUTRAS CIRCUNSTÂNCIAS PARA REVELAÇÃO DE INFORMAÇÃO**

---

As EC devem incluir na sua política de privacidade prevista no ponto 9.4, regras para permitir a divulgação de informação dos titulares das chaves, directamente aos mesmos ou a terceiros.

---

### 9.5. DIREITOS DE PROPRIEDADE INTELECTUAL

---

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID, DPC, PC e PCert, bem como qualquer outro documento, propriedade das EC pertencem à respectiva EC.

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

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

---

### 9.6. REPRESENTAÇÕES E GARANTIAS

---

---

#### 9.6.1. REPRESENTAÇÃO E GARANTIAS DAS ENTIDADES CERTIFICADORAS

---

As Entidade Certificadoras do SCEE estão obrigadas a:

- a) Realizar as suas operações de acordo com esta Política;
- b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado – DPC;
- c) Proteger as suas chaves privadas;
- d) Emitir certificados de acordo com o standard X.509;
- e) Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de *input* de dados;
- f) Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
- g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
- h) Utilizar sistemas fiáveis para armazenar certificados reconhecidos que permitam comprovar a sua autenticidade e impedir pessoas não autorizadas alterem os dados;
- i) Arquivar sem alteração os certificados emitidos;
- j) Garantir que podem determinar com precisão da data e hora em que emitiu ou extinguiu ou suspendeu um certificado;
- k) Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação;
- l) Revogar os certificados nos termos da Ponto *Suspensão e Revogação de Certificados* deste documento e publicar os certificados revogados na CRL do repositório da respectiva EC, com a frequência estipulada no ponto 4.9.7.;
- m) Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões actuais assim como as versões anteriores;
- n) Notificar com a rapidez necessária, por correio electrónico os titulares dos certificados em caso da EC proceder à revogação ou suspensão dos mesmos, indicando o

motivo que originou esta acção;

- o) Colaborar com as auditorias dirigidas pela EGCP (Autoridade Credenciadora), para validar a renovação das suas próprias chaves;
- p) Operar de acordo com a legislação aplicável;
- q) Proteger em caso de existirem as chaves que estejam sobre sua custódia;
- r) Garantir a disponibilidade da CRL de acordo com as disposições do ponto 4.9.7;
- s) Em caso de cessar a sua actividade deverá comunicar com uma antecedência mínima de dois meses a todos os titulares dos certificados emitidos assim como à ECEE;
- t) Cumprir com as especificações contidas na norma sobre Protecção de Dados Pessoais;
- u) Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante quinze anos desde o momento da emissão;
- v) Disponibilizar os certificados da sua EC e da ECRaizEstado.

---

### 9.6.2. REPRESENTAÇÃO E GARANTIAS DAS ENTIDADES DE REGISTO

---

As entidade que operam Entidades de Registo integradas na hierarquia do SCEE estão obrigadas a:

- a) Realizar suas operações de acordo com esta Política de Certificados;
- b) Realizar suas operações de acordo com as DPC da sua EC;
- c) Comprovar rigorosamente a identidade das pessoas as quais se concede o certificado digital por eles tratado, pelo que requer a presença física da pessoa;
- d) Não armazenar nem copiar os dados de criação de assinatura da pessoa a quem tenham prestado os seus serviços;
- e) Informar antes da emissão de um certificado, à pessoa que solicite seus serviços, das obrigações que assume, bem com deve guardar os dados de criação de assinatura e que procedimentos deve seguir para comunicar a perda ou utilização indevida dos dados ou dispositivos de criação ou verificação da assinatura, do seu preço, e das condições precisas para a utilização do certificado bem como das suas limitações de uso;
- f) Validar e enviar de forma segura à EC a que está subordinada a ER um pedido de certificação devidamente complementada com a informação fornecida pelo titular e assinada digitalmente e receber os certificados emitidos de acordo com esse pedido;
- g) Armazenar de forma segura até ao momento do envio, tanto a documentação fornecida pelo titular como a gerada pela própria ER durante o processo de registo ou revogação;
- h) Formalizar o Contrato de Certificação com o titular segundo o estabelecido na Declaração de Práticas;

- i) Solicitar a revogação de um certificado quando tenha conhecimento ou suspeita de compromisso de uma chave privada;
- j) Autenticar os pedidos dos utilizadores finais para a renovação ou revogação de seus certificados, gerar pedidos de renovação ou revogação assinados digitalmente e enviados a sua EC;
- k) Em caso de aprovação de um pedido de certificação, notificar o titular a emissão do certificado e a forma de obtê-lo;
- l) Em caso de negação de um pedido de certificação, notificar o titular desta recusa e o motivo da mesma;
- m) Tratando-se de certificados pessoais, deve utilizar ferramentas de pedido e envio na presença da pessoa;
- n) Manter sobre controlo restrito as ferramentas de tramitação de certificados digitais e notificar a sua EC qualquer mal funcionamento ou outra eventualidade que possa fugir ao comportamento normal;
- o) Enviar uma cópia assinada do contracto de certificação e dos seus pedidos de revogação à EC;
- p) Receber e tratar todos os pedido de revogação presenciais que receba, de forma imediata, depois de ter levar a cabo a respectiva identificação baseada no DN de quem solicita (BI, Passaporte, ...);
- q) Colaborar nos vários aspectos da operação, auditoria ou controlo da ER se tal lhe for solicitado pela EC;
- r) Obrigada a confidencialidade durante e posteriormente à prestação de serviços como Entidade de Registo, no que diz respeito à informação recebida pela EC.

---

### 9.6.3. REPRESENTAÇÃO E GARANTIAS DOS TITULARES

---

É obrigação dos titulares dos certificados emitidos:

- a) Limitar e adequar a utilização dos certificados de acordo com as utilizações previstas nas Políticas de Certificado;
- b) Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;
- c) Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado. Os moldes em que pode fazer este pedido devem estar especificados na DPC no ponto 4.9.3;
- 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) Submeter às Entidade de Registo a informação que considerem exacta e completa com relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;
- 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, de EC.

---

### **9.6.4. REPRESENTAÇÃO E GARANTIAS DAS PARTES CONFIANTES**

---

É obrigação das partes que confiem nos certificados emitidos pelas Entidade Certificadoras do Estado:

- a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na Política de Certificado correspondente;
- b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
- c) Assumir a responsabilidade na correcta verificação das assinaturas digitais;
- d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;
- e) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;
- f) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando os meios que a EC publique no seu sítio Web ([www.scee.gov.pt](http://www.scee.gov.pt)).

---

### **9.6.5. REPRESENTAÇÃO E GARANTIAS DE OUTROS PARTICIPANTES**

---

Caso existam outros participantes as DPC devem declara-las nesta secção

---

### **9.7. RENUNCIA DE GARANTIAS**

---

As EC do Estado podem recusar todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas.

---

### **9.8. LIMITAÇÕES ÀS OBRIGAÇÕES**

---

- a) As EC responderão pelos danos e prejuízos que causem a qualquer pessoa em exercício da sua actividade de acordo com o Artº 26 do DL 62/2003;
- b) As EC responderão pelos prejuízos que causem aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele;
- c) As EC assumem toda a responsabilidade mediante terceiros pela actuação dos titulares funções necessárias à prestação de serviços de certificação;
- d) A responsabilidade da administração / gestão das Entidades Certificadoras assenta sobre base objectivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;
- e) As EC só responderão pelos danos e prejuízos causados pelo uso indevido do

certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso;

- f) As EC não responderão quando o titular supere os limites que figuram no certificado quanto as suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular;
- g) As EC não responderão se o destinatário dos documentos assinados electronicamente não comprove e tenha em conta as restrições que figuram no certificado quanto às suas possíveis utilizações;
- h) As ER não assumem qualquer responsabilidade no caso de perda ou prejuízo;
- i) Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
- j) Ocasionalmente pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente DPC;
- k) Ocasionalmente pelo uso indevido ou fraudulento dos certificados ou CRL emitidos pelas EC

---

### 9.9. INDEMNIZAÇÕES

---

De acordo com a legislação em vigor

---

### 9.10. TERMO E CESSAÇÃO DA ACTIVIDADE

---

---

#### 9.10.1. TERMO

---

Esta PC entra em vigor desde o momento de sua publicação no repositório de SCEE.

Esta PC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão ou pela renovação das chaves da AC Raiz, momento em que obrigatoriamente se redigira uma nova versão.

---

#### 9.10.2. SUBSTITUIÇÃO E REVOGAÇÃO DA PC

---

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

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

### **9.10.3. CONSEQUÊNCIAS DA CESSAÇÃO DA ACTIVIDADE**

---

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

### **9.11. NOTIFICAÇÃO INDIVIDUAL E COMUNICAÇÃO AOS PARTICIPANTES**

---

Sem prejuízo do estabelecido no capítulo 4º desta PC, sobre requisitos operacionais para o ciclo de vida dos certificados, os titulares de Certificados poderão comunicar com a SCEE como entidade que tem atribuídas as competências da infra-estrutura de chave pública, através de mensagem electrónica ou por escrito através de correio postal dirigido a qualquer das direcções contidas no ponto 1.5 Administração das Políticas.

No site [www.scee.gov.pt](http://www.scee.gov.pt) estarão disponíveis outros mecanismos de contacto com a entidade competente.

As comunicações electrónicas produzirão os seus efeitos assim que as receba o destinatário ao qual vão dirigidas.

### **9.12. ALTERAÇÕES**

---

#### **9.12.1. PROCEDIMENTO PARA ALTERAÇÕES**

---

A Autoridade com atribuições para realizar e aprovar mudanças sobre esta PC é o Conselho Gestor do SCEE. Os dados de contacto do Conselho Gestor encontram-se na secção 1.5 Administração das Políticas desta PC.

#### **9.12.2. PRAZO E MECANISMO DE NOTIFICAÇÃO**

---

No caso que o Conselho Gestor julgue que as mudanças à especificação podem afectar à 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 PC no repositório estabelecido. O mecanismo de comunicação será o endereço de Internet <http://www.scee.gov.pt> e o Diário da República.

#### **9.12.3. MOTIVOS PARA MUDAR DE OID**

---

Nos casos em que, a julgamento do Conselho Gestor do SCEE, as mudanças das especificações não afectem à aceitação dos certificados proceder-se-á ao aumento do número menor de versão do documento e o último número de Identificador de objecto (OID) que o representa, mantendo o número maior da versão do documento, assim como o resto de seu OID associado. Não se considera necessário comunicar este tipo de modificações aos utilizadores dos certificados.

No caso em que o Conselho Gestor do SCEE julgue que as mudanças à especificação podem afectar à aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de objecto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 9.12.2.

---

### **9.13. DISPOSIÇÕES PARA RESOLUÇÃO DE CONFLITOS**

---

Todas reclamações entre utilizadores e SCEE deverão ser comunicadas pela parte em disputa à Entidade de Certificação Electrónica do Estado, com o fim de tentar resolvê-lo entre as mesmas partes.

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

---

### **9.14. LEGISLAÇÃO APLICÁVEL**

---

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

- a) Despacho nº 27008/2004, de 14 de Dezembro, publicado no D.R II, nº 302, de 28 de Dezembro;
- b) Portaria nº 1350/2004, de 23 de Outubro;
- c) Despacho nº 16445/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- d) Aviso nº 8134/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- e) Decreto Regulamentar nº. 25/2004, de 15 de Julho;
- f) Decreto-Lei nº 290-D/99, de 2 de Agosto com as alterações introduzidas pelo Decreto-Lei nº 62/2003, de 3 de Abril e Decreto-lei nº 165/2004, de 6 de Julho;
- g) Portaria nº 1370/2000, publicada no D.R. nº 211, II série de 12 de Setembro.

---

### **9.15. CONFORMIDADE COM A LEGISLAÇÃO EM VIGOR**

---

É responsabilidade do Conselho Gestor do SCEE zelar pelo cumprimento da legislação aplicável listada na secção 9.14

---

### **9.16. PROVIDÊNCIAS VÁRIAS**

---

---

#### **9.16.1. ACORDO COMPLETO**

---

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

---

### **9.16.2. INDEPENDÊNCIA**

---

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

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

---

### **9.16.3. SEVERIDADE**

---

Não estipulado

---

### **9.16.4. EXECUÇÕES (TAXAS DE ADVOGADOS E DESISTÊNCIA DE DIREITOS)**

---

Não estipulado

---

### **9.16.5. FORÇA MAIOR**

---

Não estipulado

---

### **9.17. OUTRAS PROVIDÊNCIAS**

---

Nada a assinalar.

### A. ANEXO - PERFIL DOS CERTIFICADOS

#### A.1. PERFIL DE CERTIFICADO DE ECRAIZESTADO

DESIGNAÇÃO (RFC3280)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption e Sha1withRsaEncryption
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=ECRaizEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	24 Anos, com renovação a cada 12 anos
4.1.2.6 Subject	Sim	CN=ECRaizEstado; O=SCEE; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSACryption, com dimensão de 4096 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Não	
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) activo(s): KeyCertSign; cRLSign
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier="AnyPolicy" com o OID: 2.5.29.32.0 e cPSuri= <a href="http://www.scee.gov.pt">http://www.scee.gov.pt</a>

4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=True e PathLenConstraint=0
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Não	
4.2.1.14 CRL Distribution Points	Não	
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
<b>Internet Certificate Extensions</b>		
4.2.2.1 Authority Information Access	Não	
4.2.2.2 Subject Information Access	Não	

### A.2. PERFIL DE CERTIFICADO DE ECESTADO

DESIGNAÇÃO (RFC3280)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption e Sha 1 withRsaEncryption
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=ECRaizEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	12 Anos, com renovação a cada 6 anos
4.1.2.6 Subject	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAAEncryption, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Sim	
4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	CRÍTICA	bit(s) activo(s): KeyCertSign; cRLSign
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier="AnyPolicy" com o OID: 2.5.29.32.0 e cPSuri=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	

4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=True e PathLenConstraint=[...]
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Não	
4.2.1.14 CRL Distribution Points	Sim	<p>“distributionPoint”= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC]</p> <p>(1) HTTP - <a href="http://crls.scee.gov.pt/crls/ARL.crl">http://crls.scee.gov.pt/crls/ARL.crl</a>;</p> <p>(2) [a DPC descreverá a existência ou não de outros pontos]</p>
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	

### Internet Certificate Extensions

4.2.2.1 Authority Information Access	Opcional	<p>accessMethod ::= {1.3.6.1.5.5.7.48.1} – “id-ad-ocsp”</p> <p>accessLocation ::= { Introduzir a localização do OCSP responder }</p>
4.2.2.2 Subject Information Access	NÃO	

### A.3. PERFIL DE CERTIFICADO DE ASSINATURA DIGITAL

DESIGNAÇÃO (RFC3280)	PERFIL	OBSERVAÇÕES
<b>Basic Certificate Fields</b>		
<b>Certificate Fields</b>		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	
4.1.1.3 signatureValue	Sim	
<b>TBSCertificate</b>		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	3 Anos
4.1.2.6 Subject	Sim	CN=[nome]; OU=[organismo]; O=[ministério]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSACryption, com dimensão mínima de 1024 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
<b>Standard Extensions</b>		
4.2.1.1 Authority Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) activo(s): nonRepudiation (contentCommitement)
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier= scee-assinatura, com o OID: [2.16.620.1.1.1.2.10] ; cPSuri=[...]; userNotice="O certificado emitido segundo esta

		política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito”
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Opção	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Não	
4.2.1.14 CRL Distribution Points	Sim	<p>“distributionPoint”= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC]</p> <p>(1) HTTP - <a href="http://crls.scee.gov.pt/crls/ARL_crl">http://crls.scee.gov.pt/crls/ARL_crl</a>;</p> <p>(2) [a DPC descreverá a existência ou não de outros pontos]</p>
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	

### Internet Certificate Extensions

4.2.2.1 Authority Information Access	Opcional	<p>accessMethod ::= {1.3.6.1.5.5.7.48.1} – “id-ad-ocsp”</p> <p>accessLocation ::= { Introduzir a localização do OCSP responder }</p>
4.2.2.2 Subject Information Access	Não	

### A.4. PERFIL DE CERTIFICADO DE AUTENTICAÇÃO

DESIGNAÇÃO (RFC3280)	PERFIL	OBSERVAÇÕES
<b>Basic Certificate Fields</b>		
<b>Certificate Fields</b>		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	
4.1.1.3 signatureValue	Sim	
<b>TBSCertificate</b>		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	3 Anos
4.1.2.6 Subject	Sim	CN=[nome];OU=[organismo];O=[ministério]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncryption, com dimensão mínima de 1024 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
<b>Standard Extensions</b>		
4.2.1.1 Authority Key Identifier	Não	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) activo(s): digitalSignature e/ou keyAgreement
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier= scee-autenticacao, com o OID: [2.16.620.1.1.1.2.20] ; cPSuri=[...]; userNotice=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	

4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opcional	
4.2.1.14 CRL Distribution Points	Sim	<p>“distributionPoint”= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC]</p> <p>(1) HTTP - <a href="http://crls.scee.gov.pt/crls/ARL.crl">http://crls.scee.gov.pt/crls/ARL.crl</a>;</p> <p>(2) [a DPC descreverá a existência ou não de outros pontos]</p>
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	

### Internet Certificate Extensions

4.2.2.1 Authority Information Access	Opcional	<p>accessMethod ::= {1.3.6.1.5.5.7.48.1} – “id-ad-ocsp”</p> <p>accessLocation ::= { Introduzir a localização do OCSP responder }</p>
4.2.2.2 Subject Information Access	Não	

**A.5. PERFIL DE CERTIFICADO DE CONFIDENCIALIDADE**

DESIGNAÇÃO (RFC3280)	PERFIL	OBSERVAÇÕES
<b>Basic Certificate Fields</b>		
<b>Certificate Fields</b>		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	
4.1.1.3 signatureValue	Sim	
<b>TBSCertificate</b>		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	3 Anos
4.1.2.6 Subject	Sim	CN=[nome];OU=[organismo];O=[ministério]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSACryption, com dimensão mínima de 1024 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
<b>Standard Extensions</b>		
4.2.1.1 Authority Key Identifier	Não	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) activo(s): keyEncipherment e/ou keyAgreement
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier=scee-confidencialidade, com o OID: 2.16.620.1.1.1.2.30 ; cPSuri=[...]; userNotice=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Não	

4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opcional	
4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
<b>Internet Certificate Extensions</b>		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::= {1.3.6.1.5.5.7.48.1} – "id-ad-ocsp" accessLocation ::= { Introduzir a localização do OCSP responder }
4.2.2.2 Subject Information Access	Não	

**B. ANEXO – PERFIL DAS LCR**

DESIGNAÇÃO (RFC3280)	PERFIL	OBSERVAÇÕES
CertificateList Fields		
5.1.1.1 tbsCertList		
5.1.1.2 signatureAlgorithm	Sim	
5.1.1.3 signatureValue	Sim	
tbsCertList		
5.1.2.1 Version	Sim	
5.1.2.2 Signature	Sim	
5.1.2.3 Issuer Name	Sim	
5.1.2.4 This Update	Sim	
5.1.2.5 Next Update	Sim	
5.1.2.6 Revoked Certificates	Sim	
5.1.2.7 Extensions	Sim	
CRL Extensions		
5.2.1 Authority Key Identifier	Sim	
5.2.2 Issuer Alternative Name	Não	
5.2.3 CRL Number	Sim	
5.2.4 Delta CRL Indicator	Não	
5.2.5 Issuing Distribution Point	Não	
5.2.6 Freshest CRL	Não	
CRL Entry Extensions		
5.3.1 Reason Code	Sim	
5.3.2 Hold Instruction Code	Não	
5.3.3 Invalidity Date	Não	
5.3.4 Certificate Issuer	Não	

## C. ANEXO – NORMALIZAÇÃO TÉCNICA

X.501	<p>Nome: ITU-T RECOMMENDATION X.501   ISO/IEC 9594-2:2001</p> <p>Versão: —</p> <p>Tipo: Recommendation</p> <p>Data: Fevereiro de 2001</p> <p>Organismo: International Telecommunications Union</p> <p>Descrição: Information technology - Open Systems Interconnection - The Directory: Models</p>
RFC3647	<p>Nome: RFC 3647</p> <p>Versão: Torna obsoleto o RFC 2527</p> <p>Tipo: Request For Comments</p> <p>Data: Novembro de 2003</p> <p>Organismo: Internet Engineering Task Force - PKIX Working Group</p> <p>Descrição: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework</p>
RFC3280	<p>Nome: RFC 3280</p> <p>Versão: Torna obsoleto o RFC 2459 e é actualizado pelo RFC 4325</p> <p>Tipo: Request For Comments</p> <p>Data: Abril de 2002</p> <p>Organismo: Internet Engineering Task Force - PKIX Working Group</p> <p>Descrição: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL).</p>
RFC 4325	<p>Nome: RFC 4325</p> <p>Versão: Actualiza o RFC 3280</p> <p>Tipo: Request For Comments</p> <p>Data: Dezembro de 2005</p> <p>Organismo: Internet Engineering Task Force - PKIX Working Group</p> <p>Descrição: Internet X.509 Public Key Infrastructure - Authority Information Access Certificate Revocation List (CRL) Extension</p>
RFC3161	<p>Nome: RFC 3161</p> <p>Versão: —</p> <p>Tipo: Request For Comments</p> <p>Data: Agosto de 2001</p>

	<p>Organismo: Internet Engineering Task Force - PKIX Working Group</p> <p>Descrição: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)</p>
RFC2560	<p>Nome: RFC 2560</p> <p>Versão: —</p> <p>Tipo: Request For Comments</p> <p>Data: Junho de 1999</p> <p>Organismo: Internet Engineering Task Force - PKIX Working Group</p> <p>Descrição: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP</p>
RFC2510	<p>Nome: RFC 2510</p> <p>Versão: —</p> <p>Tipo: Request For Comments</p> <p>Data: Março 1999</p> <p>Organismo: Internet Engineering Task Force - PKIX Working Group</p> <p>Descrição: Internet X.509 Public Key Infrastructure - Certificate Management Protocols</p>
X.509	<p>Nome: ITU-T Recommendation X.509 (08/05)   ISO/IEC 9594-8</p> <p>Versão: —</p> <p>Tipo: Recommendation</p> <p>Data: Agosto de 2005</p> <p>Organismo: International Telecommunications Union</p> <p>Descrição: Information Technology – Open Systems Interconnection - The Directory: Authentication Framework</p>
ISO17799	<p>Nome: ISO/IEC 17799:2005</p> <p>Versão: Actualiza a ISO/IEC 17799:2000</p> <p>Tipo: International Standard</p> <p>Data: Junho de 2005</p> <p>Organismo: International Organization for Standardization e International Electrotechnical Commission</p> <p>Descrição: Information technology - Security techniques - Code of practice for information security management</p>
ISO15408-3	<p>Nome: ISO/IEC 15408-3:2005</p> <p>Versão: 2ª Edição</p> <p>Tipo: International Standard</p>

	<p><b>Data:</b> Outubro de 2005</p> <p><b>Organismo:</b> International Organization for Standardization) e International Electrotechnical Commission</p> <p><b>Descrição:</b> Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements</p>
ISO15408-2	<p><b>Nome:</b> ISO/IEC 15408-1:2005</p> <p><b>Versão:</b> 2ª Edição</p> <p><b>Tipo:</b> International Standard</p> <p><b>Data:</b> Outubro de 2005</p> <p><b>Organismo:</b> International Organization for Standardization) e International Electrotechnical Commission</p> <p><b>Descrição:</b> Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements</p>
ISO15408-1	<p><b>Nome:</b> ISO/IEC 15408-1:2005</p> <p><b>Versão:</b> 2ª Edição</p> <p><b>Tipo:</b> International Standard</p> <p><b>Data:</b> Outubro de 2005</p> <p><b>Organismo:</b> International Organization for Standardization) e International Electrotechnical Commission</p> <p><b>Descrição:</b> Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model</p>
ISO9595	<p><b>Nome:</b> ISO/IEC 9595</p> <p><b>Versão:</b> 4ª correcção</p> <p><b>Tipo:</b> International Standard</p> <p><b>Data:</b> 1998</p> <p><b>Organismo:</b> International Organization for Standardization e International Electrotechnical Commission</p> <p><b>Descrição:</b> Information technology - Open Systems Interconnection - Common management information Service definition"</p>
ISO9564-1	<p><b>Nome:</b> ISO 9564-1:</p> <p><b>Versão:</b> Actualiza a versão de 1991</p> <p><b>Tipo:</b> International Draft</p> <p><b>Data:</b> Maio de 2002</p> <p><b>Organismo:</b> International Organization for Standardization</p> <p><b>Descrição:</b> Banking - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems</p>

ISO9564-2	<p>Nome: ISO 9564-2</p> <p>Versão: Actualiza a versão de 1991</p> <p>Tipo: International Draft</p> <p>Data: Janeiro de 2005</p> <p>Organismo: International Organization for Standardization</p> <p>Descrição: Banking – Personal Identification Number management and security – Part 2: Approved algorithms for PIN encipherment</p>
ISO9564-3	<p>Nome: ISO 9564-3</p> <p>Versão: —</p> <p>Tipo: International Draft</p> <p>Data: Novembro de 2003</p> <p>Organismo: International Organization for Standardization</p> <p>Descrição: Banking – Personal Identification Number management and security – Part 3: Requirements for offline PIN handling in ATM and POS systems</p>
ISO3166-1	<p>Nome: ISO 3166-1</p> <p>Versão: —</p> <p>Tipo: International Draft</p> <p>Data: Julho de 2003</p> <p>Organismo: International Organization for Standardization</p> <p>Descrição: Code lists - country names and code elements - alpha-2 code elements</p>
ISO 11568-1	<p>Nome: ISO 11568-1</p> <p>Versão: —</p> <p>Tipo: International Standard</p> <p>Data: 2005</p> <p>Organismo: International Organization for Standardization</p> <p>Descrição: Banking – Key management (retail) - Part 1: Principles</p>
ISO 11568-2	<p>Nome: ISO 11568-2</p> <p>Versão: —</p> <p>Tipo: International Standard</p> <p>Data: 2005</p> <p>Organismo: International Organization for Standardization</p> <p>Descrição: Banking – Key management (retail) – Part 2: Symmetric ciphers, their key management and life cycle</p>
ISO 11568-4	<p>Nome: ISO 11568-4</p>

	<p>Versão: —</p> <p>Tipo: International Standard</p> <p>Data: 1998</p> <p>Organismo: International Organization for Standardization</p> <p>Descrição: Banking – Key management (retail) – Part 4: Key management techniques using public key cryptosystems</p>
ISO11568-5	<p>Nome: ISO 11568-5</p> <p>Versão: —</p> <p>Tipo: International Standard</p> <p>Data: 2005</p> <p>Organismo: International Organization for Standardization</p> <p>Descrição: Banking – Key management (retail) – Part 5: Key life cycle for public key cryptosystems</p>
FIPS140-2	<p>Nome: FIPS PUB 140-2</p> <p>Versão: Actualiza o FIPS PUB 140-1 de Janeiro de 1994</p> <p>Tipo: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION</p> <p>Data: Março 2002</p> <p>Organismo: US National Institute of Standards and Technology</p> <p>Descrição: "Security Requirements For Cryptographic Modules".</p>
ETSI102280	<p>Nome: ETSI TS 102 280</p> <p>Versão: V1.1.1</p> <p>Tipo:</p> <p>Data: Março de 2004</p> <p>Organismo:</p> <p>Descrição: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons</p>
ETSI102176-1	<p>Nome: ETSI TS 102 176- 1</p> <p>Versão: V1.2.1</p> <p>Tipo:</p> <p>Data: Julho de 2005</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Part 1 - Algorithms and Parameters for Secure Electronic Signatures;</p>
ETSI102176-2	<p>Nome: ETSI TS 102 176- 2</p> <p>Versão: V1.2.1</p> <p>Tipo:</p>

	<p>Data: Julho de 2005</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Part 2: Secure channel protocols and algorithms for signature creation devices</p>
ETSI102158	<p>Nome: ETSI TS 102 158</p> <p>Versão: V1.1.1</p> <p>Tipo:</p> <p>Data: Outubro de 2003</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates</p>
ETSI102042	<p>Nome: ETSI TS 102 042</p> <p>Versão: V1.2.2</p> <p>Tipo:</p> <p>Data: Junho de 2005</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Policy requirements for certification authorities issuing public key certificates</p>
ETSI102042	<p>Nome: ETSI TS 102 042</p> <p>Versão: 1.2.2</p> <p>Tipo: Technical Specification</p> <p>Data: Junho de 2005</p> <p>Organismo: ESI - Electronic Signatures and Infrastructures</p> <p>Descrição: Policy Requirements for certification authorities issuing public key certificates</p>
ETSI102023	<p>Nome: ETSI TS 102 023</p> <p>Versão: V1.2.1</p> <p>Tipo: Technical Specification</p> <p>Data: Janeiro de 2003</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Policy requirements for time-stamping authorities</p>
ETSI101903	<p>Nome: ETSI TS 101 903</p> <p>Versão: V1.3.2</p> <p>Tipo: Technical Specification</p> <p>Data: Março de 2006</p>

	<p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: XML Advanced Electronic Signatures (XAdES)</p>
ETSI101862	<p>Nome: ETSI TS 101 862</p> <p>Versão: V1.3.3</p> <p>Tipo: Technical Specification</p> <p>Data: Janeiro de 2006</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Qualified Certificate profile</p>
ETSI101862	<p>Nome: ETSI TS 101 862</p> <p>Versão:</p> <p>Tipo:</p> <p>Data:</p> <p>Organismo:</p> <p>Descrição:</p>
ETSI101861	<p>Nome: ETSI TS 101 861</p> <p>Versão: V1.3.1</p> <p>Tipo: Technical Specification</p> <p>Data: Janeiro de 2006</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Time stamping profile</p>
ETSI101733	<p>Nome: ETSI TS 101 733</p> <p>Versão: V1.6.3</p> <p>Tipo: Technical Specification</p> <p>Data: Setembro de 2005</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: CMS Advanced Electronic Signatures (CAdES)</p>
ETSI101456	<p>Nome: ETSI TS 101 456</p> <p>Versão: V1.4.1</p> <p>Tipo: Technical Specification</p> <p>Data: Janeiro de 2006</p> <p>Organismo: Electronic Signatures and Infrastructures (ESI);</p> <p>Descrição: Policy requirements for certification authorities issuing qualified certificates</p>

CWA15264-3	<p>Nome:</p> <p>Versão:</p> <p>Tipo: Abril 2005</p> <p>Data:</p> <p>Organismo:</p> <p>Descrição: User Requirements for a European interoperable eID system within a smart card infrastructure</p>
CWA15264-2	<p>Nome:</p> <p>Versão:</p> <p>Tipo:</p> <p>Data: Abril 2005</p> <p>Organismo:</p> <p>Descrição: Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services</p>
CWA15264-1	<p>Nome:</p> <p>Versão:</p> <p>Tipo:</p> <p>Data: Abril 2005</p> <p>Organismo:</p> <p>Descrição: Architecture for a European interoperable eID system within a smart card infrastructure</p>
CWA14890-2	<p>Nome: CWA 14890-2</p> <p>Versão:</p> <p>Tipo:</p> <p>Data:</p> <p>Organismo:</p> <p>Descrição: Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services</p>
CWA14890-1	<p>Nome: CWA 14890-1</p> <p>Versão:</p> <p>Tipo:</p> <p>Data:</p> <p>Organismo:</p>

	<p><b>Descrição:</b> Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements</p>
CWA14365-2	<p><b>Nome:</b> CWA 14365-2</p> <p><b>Versão:</b></p> <p><b>Tipo:</b> CEN Workshop Agreement</p> <p><b>Data:</b></p> <p><b>Organismo:</b> European Committee for Standardization</p> <p><b>Descrição:</b> Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices</p>
CWA14365-1	<p><b>Nome:</b> CWA 14365-1</p> <p><b>Versão:</b></p> <p><b>Tipo:</b> CEN Workshop Agreement</p> <p><b>Data:</b></p> <p><b>Organismo:</b> European Committee for Standardization</p> <p><b>Descrição:</b> Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects</p>
CWA14355	<p><b>Nome:</b> CWA 14355</p> <p><b>Versão:</b></p> <p><b>Tipo:</b> CEN Workshop Agreement</p> <p><b>Data:</b> Março de 2004</p> <p><b>Organismo:</b> European Committee for Standardization</p> <p><b>Descrição:</b> Guidelines for the implementation of Secure Signature-Creation Devices</p>
CWA14172-8	<p><b>Nome:</b> CWA 14172-8</p> <p><b>Versão:</b></p> <p><b>Tipo:</b> CEN Workshop Agreement</p> <p><b>Data:</b></p> <p><b>Organismo:</b> European Committee for Standardization</p> <p><b>Descrição:</b> EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes</p>
CWA14172-7	<p><b>Nome:</b> CWA 14172-7</p> <p><b>Versão:</b></p> <p><b>Tipo:</b> CEN Workshop Agreement</p>

	<p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services</p>
CWA14172-6	<p>Nome: CWA 14172-6</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified</p>
CWA14172-5	<p>Nome: CWA 14172-5</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices</p>
CWA14172-4	<p>Nome: CWA 14172-4</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification</p>
CWA14172-3	<p>Nome: CWA 14172-3</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures</p>
CWA14172-2	<p>Nome: CWA 14172-2</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p>

	<p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes</p>
CWA14172-1	<p>Nome: CWA 14172-1</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: EESSI Conformity Assessment Guidance - Part 1: General introduction</p>
CWA14171	<p>Nome: CWA 14171</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data: Maio de 2004</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: General guidelines for electronic signature verification</p>
CWA14170	<p>Nome: CWA 14170</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data: Maio de 2004</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: Security requirements for signature creation applications</p>
CWA14169	<p>Nome: CWA 14169</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data: Março de 2004</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: Secure signature-creation devices "EAL 4+"</p>
CWA14167-4	<p>Nome: CWA 14167-4</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing</p>

	operations - Protection profile - CMCSO PP
CWA14167-3	<p>Nome: CWA 14167-3</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)</p>
CWA14167-2	<p>Nome: CWA 14167-2</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)</p>
CWA14167-1	<p>Nome: CWA 14167-1</p> <p>Versão:</p> <p>Tipo: CEN Workshop Agreement</p> <p>Data:</p> <p>Organismo: European Committee for Standardization</p> <p>Descrição: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements</p>
CCMB3	<p>Nome: CCMB-2005-08-003</p> <p>Versão: V 2.3</p> <p>Tipo:</p> <p>Data: Agosto de 2005</p> <p>Organismo:</p> <p>Descrição: Common Criteria for Information Technology Security Evaluation Part 3: Security assurance</p>
CCMB2	<p>Nome: CCMB-2005-08-002</p> <p>Versão: V 2.3</p> <p>Tipo:</p> <p>Data: Agosto de 2005</p> <p>Organismo:</p>

	<b>Descrição:</b> Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements
CCMB1	<b>Nome:</b> CCMB-2005-08-001 <b>Versão:</b> V 2.3 <b>Tipo:</b> <b>Data:</b> Agosto de 2005 <b>Organismo:</b> <b>Descrição:</b> Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model

### D. ANEXO – DEFINIÇÕES E ACRÓNIMOS

---

Com o objectivo de conhecer os conceitos que são utilizados no presente documento e nas diferentes Declarações de Práticas de Certificação deve entender-se:

#### D.1. ACRÓNIMOS

---

AdmHSM	Administradores do HSM
AdmReg	Administrador de registo
AdmSeg	Administrador de Segurança
AdmSist	Administrador de Sistemas
AuditorS	Auditor de Sistemas
AV	Autoridades de Validação
C	Country
CEN	Comité Européen de Normalisation
CMP	Certificate Management Protocols
CMP	Certificate Management Protocol
CN	Common Name
CSP	Cryptographic Service Provider Microsoft
CWA	CEN Workshop Agreement
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EC	Entidade Certificadora
SCEE	Sistema de Certificação Electrónica do Estado
ECEstado	Entidade Certificadora do Estado
ECRaizEstado	Entidade Certificadora de Raiz do Estado
ER	Entidade de registo
EREstado	Entidade de Registo do Estado
ETSI	European Telecommunications Standard Institute

FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module.
ICP	Infra-Estrutura de Chave Pública
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IETF	Internet Engineering Task Force
LCR	Lista de Certificados Revogados
LDAP	Lightweight Directory Access Protocol
LER	Lista de Certificados de Entidades Certificadoras Revogadas
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OpHSM	Operadores do HSM
OpSist	Operador de Sistemas
OU	Organizacional Unit
P1	Perfil de Certificado de ECRaizEstado;
P2	Perfil de Certificado de ECEstado;
P3	Perfil de Certificado de Assinatura Digital;
P4	Perfil de Certificado de Autenticação;
P5	Perfil de Certificado de Confidencialidade;
P6	Perfil de Certificado de Time Stamping;
P7	Perfil de Certificado de OCSP.
PC	Política de Certificado
PCert	Política de Certificados da SCEE
PED	PIN Entry Device
PKCS	Public-Key Cryptography Standards
PKCS#1	RSA Cryptography Standard

PKCS#10	Certification Request Syntax Standard
PKCS#11	Cryptographic Token Interface Standard
PKCS#7	Cryptographic Message Syntax Standard
RAF	relatório de auditoria final
RCI	relatório de correcção de irregularidades
RFC	Request For Comments
RPI	relatório de primeiras impressões
RSA	Algoritmo criptográfico (Rivest   Shamir   Adleman)
RSAE	Relatório Sumário de Análise de Eventos
subECEstado	Entidade Certificadora Subordinada dum ECEstado
TCP/IP	Transmission Control Protocol/Internet Protocol
TRT	Termo de Responsabilidade do Titular
OID	Identificador de Objecto
URL	Unified Resource Locator

---

## D.2. DEFINIÇÕES

---

Assinatura digital	Modalidade de assinatura electrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura;
Assinatura electrónica avançada	Assinatura electrónica que preenche os seguintes requisitos: <ul style="list-style-type: none"> <li>i) Identifica de forma unívoca o titular como autor do documento;</li> <li>ii) A sua aposição ao documento depende apenas da vontade do titular;</li> <li>iii) É criada com meios que o titular pode manter sob seu controlo exclusivo;</li> <li>iv) A sua conexão com o documento permite detectar toda e qualquer</li> </ul>

	alteração superveniente do conteúdo deste;
Assinatura electrónica qualificada	Assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura;
Assinatura electrónica	É o resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico.
Autoridade credenciadora	Entidade competente para a credenciação e fiscalização das entidades credenciadoras;
C	Atributo do DN de um objecto dentro da estrutura de directório X.500.
Certificado	Estrutura de dados assinado electronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento electrónico, ou se decifra um documento electrónico previamente cifrado com a correspondente chave pública;
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves;
Chave	Sequencia de símbolos
CN	Atributo do DN de um objecto dentro da estrutura de directório X.500.
Credenciação	Acto pelo qual é reconhecido a uma entidade que o solicite e que exerça a actividade de entidade credenciadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos;
Dados de Activação	Dados privados, diferentes das chaves, exigidos para o acesso aos módulos criptográficos.
Dados de criação de assinatura	São dados únicos, como códigos ou chaves criptográficas privadas que o titular utiliza para gerar a sua assinatura electrónica.
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura electrónica;

Dados de verificação de assinatura	São dados como códigos ou chaves criptográficas públicas, que se utilizam para verificar a assinatura electrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura electrónica;
Declaração de Práticas de Certificação	Documento onde são especificados ao pormenor a forma como Prestador de Serviços de Certificação realiza as actividades relacionadas com a gestão do ciclo de vida do certificado
Directório de Certificados:	Repositório de informação que segue o standard X500
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura;
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que:  i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada;  ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis;  iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros;  iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura;
DN	Identificação unívoca de uma entrada dentro da estrutura de directório X.500.
Documento Electrónico	Conjunto de dados lógicos armazenados em suporte susceptível de poder ser lido por equipamentos electrónicos de processamento de dados.
Endereço electrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos.
Entidade certificadora	Entidade ou pessoa singular ou colectiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respectiva publicidade e presta outros serviços relativos a assinaturas electrónicas;

Entidade de Registo	Entidade ou pessoa singular ou colectiva designada pelas Entidades Certificadoras para realizar actividades de comprovação da identidade dos subscritores ou titulares e conseqüente registo, bem como a gestão de pedidos de revogação de certificados.
Função hash	É uma operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados iniciais e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função.
Hash ou impressão digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais.
HSM	Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.
Infra-Estrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico.
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas.
LER	Lista de certificados de outras CA revogados. Uma ARL é equivalente a uma CRL para os certificados cruzados com outras CA.
Módulo Criptográfico Hardware	módulo de hardware utilizado para realizar funções criptográficas e armazenar chaves em modo seguro.
Número de série de Certificado	valor inteiro e único que está associado inequivocamente com um certificado emitido pela SCEE.
O	Atributo do DN de um objecto dentro da estrutura de directório X.500.
OCSP	protocolo que permite a comprovação do estado do certificado no momento em que o mesmo é utilizado.
OCSP Responder	Servidor que responde segundo o protocolo OCSP aos pedidos OCSP com o estado do certificado.
OID	O identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objecto específico ou a uma classe de objectos específica.
OU	Atributo do DN de um objecto dentro da estrutura de directório X.500.

Pedido OCSP	pedido de consulta de estado de um certificado a um OCSP Responder.
PIN	Personal Identification Number
PIN	número específico apenas conhecido pela pessoa que tem de aceder a um recurso que se encontra protegido por este mecanismo.
PKCS	Conjunto de standard desenvolvido pela RSA Labs aceite internacionalmente para definição da sintaxe a utilizar com a criptografia de chave pública.
PKIX	Grupo de trabalho do IETF constituído para desenvolver as especificações relacionadas com PKI e Internet.
Time Stamping	Constatação da data e hora de um documento electrónico mediante processos criptográficos, para datar os documentos de forma objectiva.
SHA	Desenvolvido pelo NIST e revisto em 1994 (SHA-1). Este algoritmo consiste em transformar mensagens de menos de 264 bits e gerar um resumo de 160 bits de comprimento. A probabilidade de encontrar duas mensagens distintas que produzam o mesmo resumo é praticamente nula, por esse motivo utiliza-se para assegurar a integridade dos documentos durante o processo de assinatura electrónica.
SmartCard	Cartão criptográfico utilizado pelo titular para armazenar chaves privadas de assinatura e ou cifra. Os smartcards são considerados dispositivos seguros de criação de assinatura e de acordo com a lei permite a geração de assinatura electrónica qualificadas.
Titular	Pessoa singular ou colectiva identificada num certificado como a detentora de um dispositivo de criação de assinatura;
Validação cronológica	declaração de entidade certificadora que atesta a data e hora da criação, expedição ou recepção de um documento electrónico;
X.500	Standard desenvolvido pelo ITU que define as recomendações de um directório. Corresponde ao standard ISO 9594-1
X.509	Standard desenvolvido pelo ITU que define o formato electrónico dos certificados electrónicos.
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios electrónicos.

**E. ANEXO – HIERARQUIA DE OID DA SCEE**

CONSTRUÇÃO DO OID					DESCRIÇÃO
0					Testes/experimental
1					Objectos Relacionados com a PKI do SCEE {id-pki-scee }
1	1				Objectos relacionados com a identificação de entidades
1	1	1			ECRaizEstado
1	1	1	m		m-ésimo processo de renovação
1	1	2			Entidades Certificadoras do Estado (ECEstado)
1	1	2	n		ECEstado n
1	1	2	n	m	subECEstado
1	1	3			Entidade de Registo do Estado (EREstado)
1	1	3	n		EREstado n
1	1	3	n	m	processo de renovação m-ésimo
1	1	100			Outros objectos relacionados com a identificação de entidades da comunidade SCEE-ICP.
1	2				Objectos relacionados com Politicas de Certificados

1	2	1			SCEE Políticas de Certificado
1	2	1	V	v	Política de Certificados do SCEE (Versão V.v)
1	2	10			Política de Certificado para Assinatura Digital
1	2	20			Política de Certificado para Autenticação
1	2	30			Política de Certificado para Confidencialidade